Personnel Safety System Generation-3 Review April 26-27, 2004

Presented by

K. Belcher, A. Boron, J. Carwardine, R. Emerson, M. Fagan, N. Friedman, G. Markovich, V. Nguyen, J. Servino

Argonne National Laboratory

Office of Science
U.S. Department of Energy

A U.S. Department of Energy
Office of Science Laboratory
Operated by The University of Chicago

Agenda
Monday, April 26, 2004

8:30am - Charge to committee (J. Carwardine)

8:40am - An overview of the APS / beamlines / safety systems (M. Knott)

8:50am - Overview of existing PSS Gen-1 systems and rationale (J. Hawkins)

9:30am - Goals, Migration Justification and Feature comparison Gen-3 (R. Emerson)

10:30am - Break

10:45am - Non-invasive testing methodology (M. Fagan)

11:30am - Gen-3 hardware design (K. Belcher)

12:30pm - Lunch

1:45pm - Tour - 4-ID (N. Friedman)

2:30pm - Gen-3 software design (R. Emerson)

3:00pm - PSS Chain-A (A. Boron)

3:30pm - PSS Chain-B (V. Nguyen)

4:00pm - PSS Chain-C, HMI and EPICS (J. Servino)

4:45pm - Validation System (V. Nguyen)

5:00pm - Laboratory Simulator (A. Boron)

5:15pm - Retrofitting key Gen-3 functionality to existing Gen-1 systems (R. Emerson)

5:30pm - Gen-3 Goals – What was presented to meet them (R. Emerson)

5:45pm - Done

6:15pm - Dinner at Argonne Guest House

Agenda
Tuesday, April 27, 2004

8:30am	**-**	**Gen-3 prototype implementation at 30-ID (R. Emerson)**
9:15am	**-**	**Training on the new functionality and testing methods (G. Markovich)**
9:30am	**-**	**Approvals & Processes (R. Emerson)**
9:40am	**-**	**From Prototype to Production, The Standard Build Package (G. Markovich)**
10:00am	**-**	**Break**
10:15am	**-**	**Open for questions and additional topics as requested by review committee members.**
12:00pm	**-**	**Review committee working lunch to create draft report.**
2:30pm	**-**	**Close-out**

Charge to Committee

John Carwardine

Review committee members

- Mohan Ramanathan AOD (Chair), mohan@aps.anl.gov
- Paul C. Czarapata, FNAL Beams Division, pcceed@fnal.gov
- John Forrestal, ASD Safety Interlocks Group, jrf@aps.anl.gov
- Nick Friedman, ASD Safety Interlocks Group, friedman@aps.anl.gov
- Jon Hawkins, ASD Safety Interlocks Group, hawkins@aps.anl.gov
- Martin J. Knott, ASD Electrical Systems, mjk@aps.anl.gov
- James Lang, ASD, Chair, APS Radiation Safety Policy Committee jwl@aps.anl.gov
- Jonathan Lang, XFD XOR, lang@aps.anl.gov
- Kelly Mahoney, Jefferson Lab Interlock Safety Systems, mahoney@jlab.org
- Tom Barsz, ASD QA Representative, tbarsz@aps.anl.gov

Charge to the committee

- **Assess the philosophy, design, and implementation of PSS Generation-3 as a new standard for future beamlines.**

- **Specifically, we request you do the following**
  - Assess whether the goals and objectives from the statement of work have been adequately addressed.
  - Review, at a high level, testing methods, and plans to migrate towards semi-automated periodic testing.
  - Give readiness go/no-go approval for implementation of a prototype Generation-3 system at 30-ID.

- **Out of scope for this review**
  - All previously reviewed design features and implementation for the existing PSS Generation-1 systems.

Reviewer comments

- **We request that you rank committee comments, as follows**
  - "Best practice / good solution“
  - "Non-negotiable" changes to the philosophy, design, or implementation.
  - "Strongly recommended" changes to the philosophy, design, or implementation.
  - "Suggested" changes to the philosophy, design, or implementation.
  - "Other comments”

- **We request that you present your assessment in an exit interview, followed by a written report within 7 days.**

QUESTIONS?

Overview of the APS, its Beamlines and Safety Systems

- *a Primer*

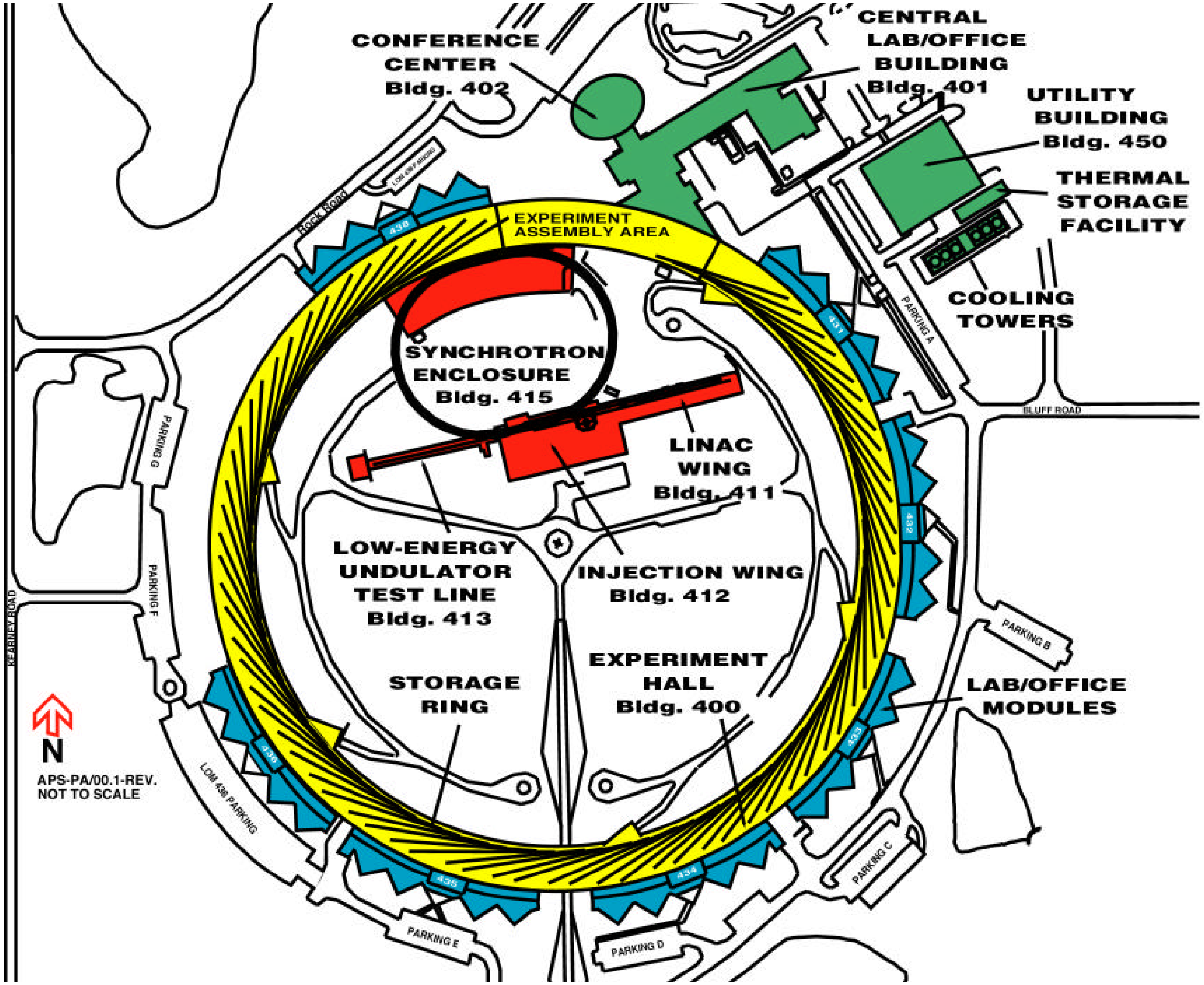
Marty Knott

Electrical Systems

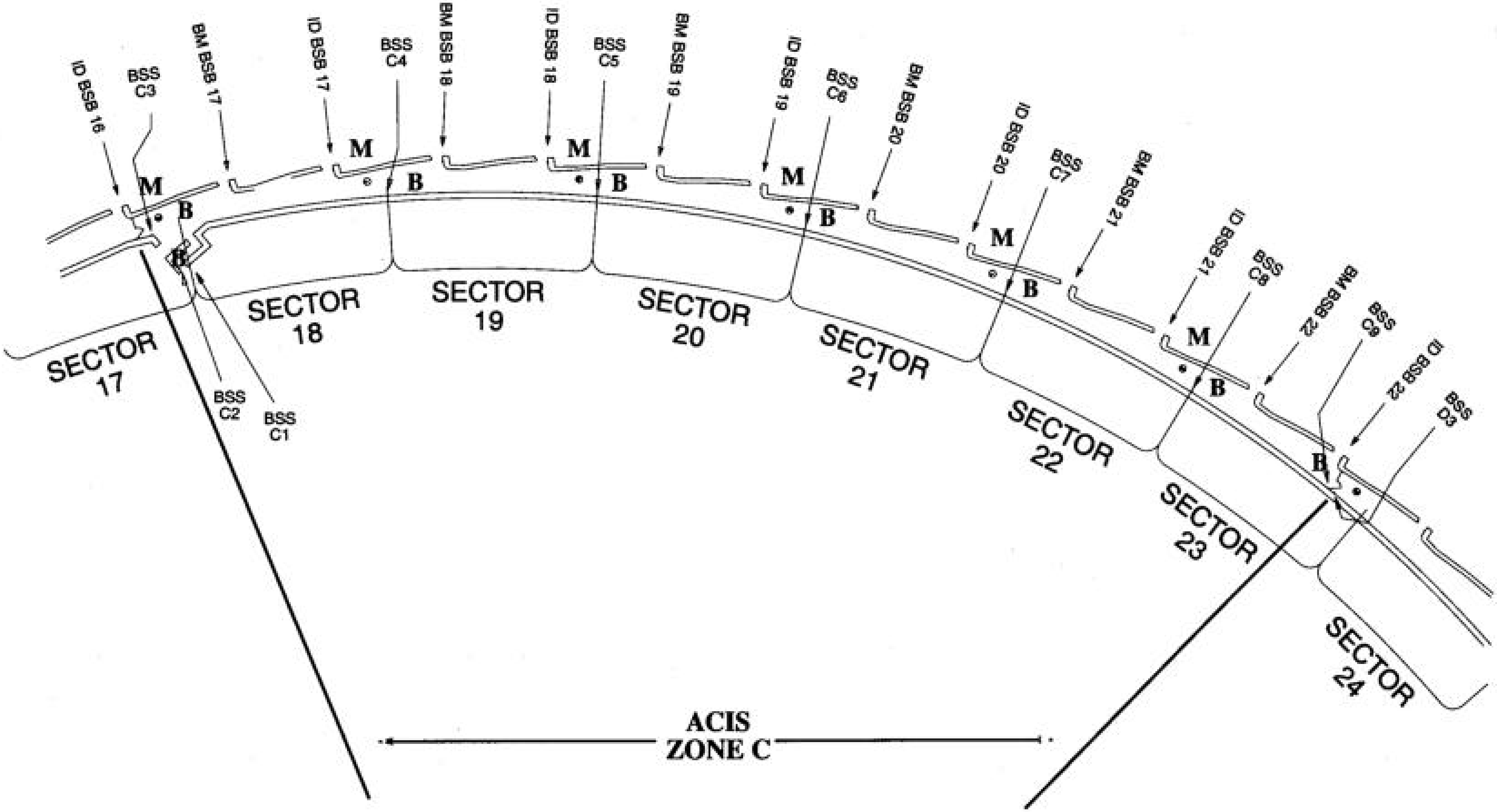
Overview of APS

- **The Advanced Photon Source is a chain of four accelerators:**
  - 400 MeV linac
  - Particle accumulator and compression ring (PAR)
  - 7 GeV synchrotron (booster)
  - 7 Gev storage ring
  - The low energy undulator test line (LEUTL) is a separate facility utilizing the linac beam.
- **Each is separated with shield walls and beam stopping devices.**
- **Each has a dedicated personnel safety system, the Access Control Interlock Systems (ACIS) implemented with dual PLCs. (The storage ring employs two ACISs.)**

Plan view of the Advanced Photon Source

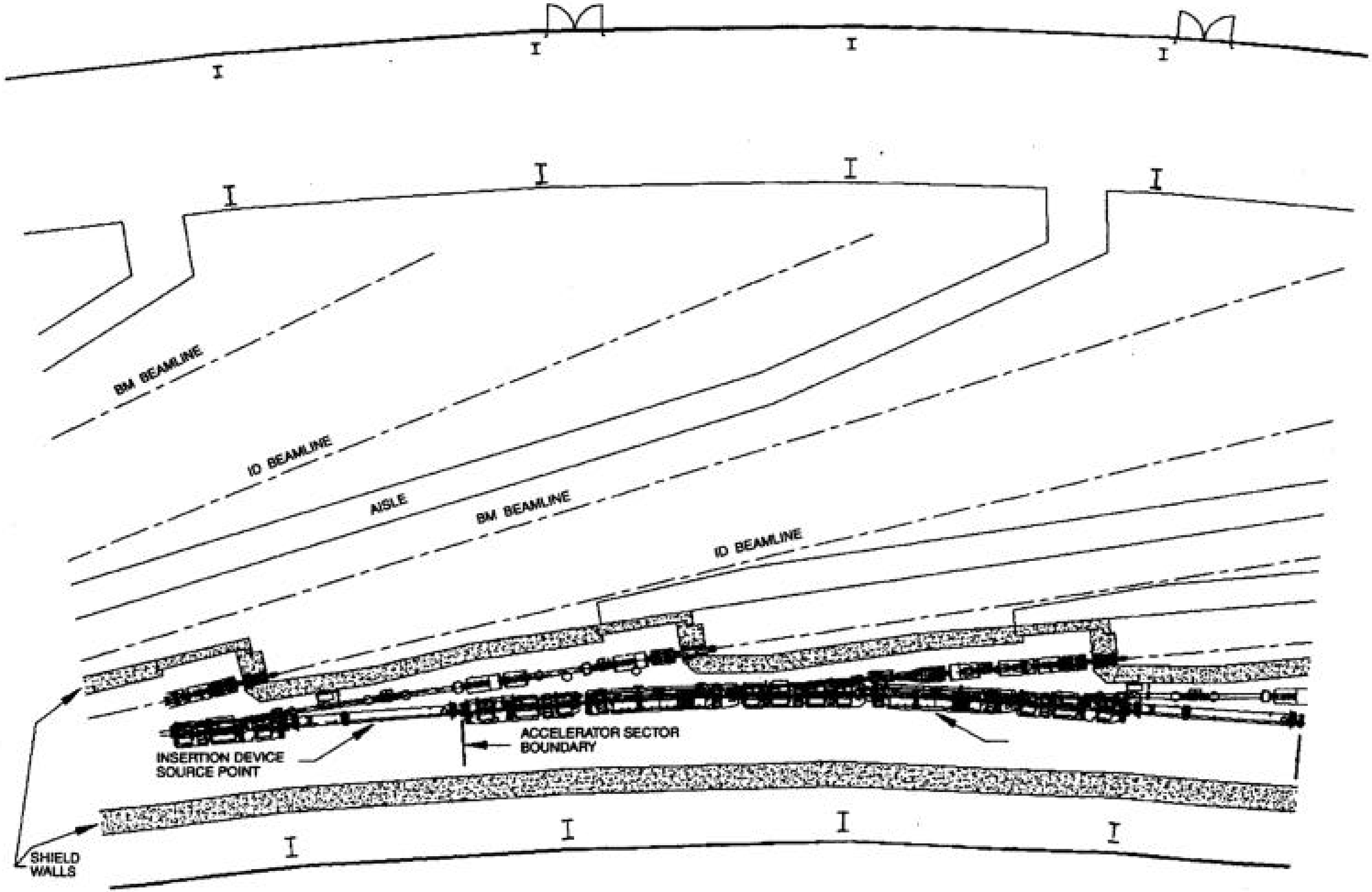


Location of storage ring Zone-C ACIS equipment

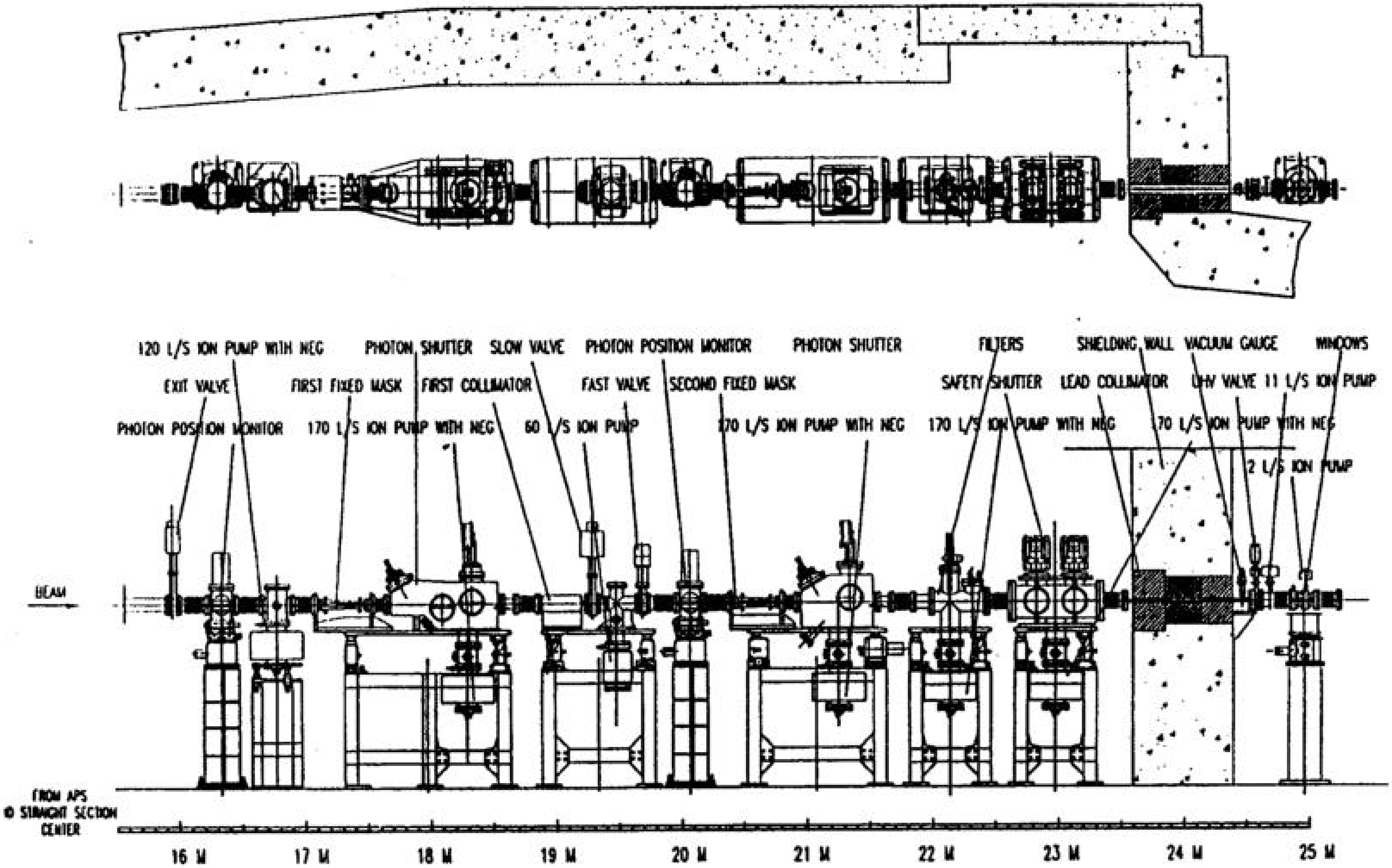


Key: B..........Beam Shutdown Station
M.........Radiation Monitor Location

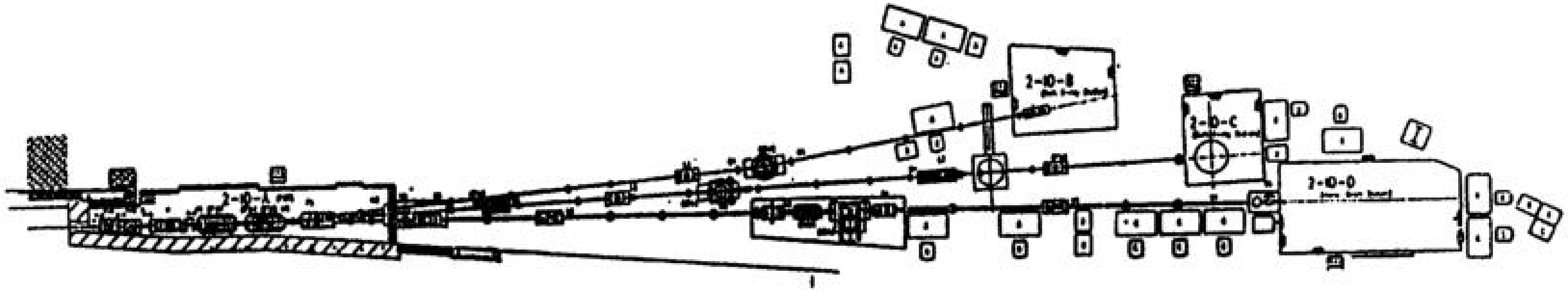
Sector layout of storage ring in-tunnel components



Typical front-end layout



Layout of a typical insertion device beamline



Overview of the APS Interlock Systems

- **Each of the 70 potential photon beamlines has a dedicated Personnel Safety System (PSS) implemented with dual PLCs.**
- **ACIS/PSS Common Aspects:**
  - Stand-alone operation
  - Independent validation
  - Minimal signal exchange (Trip, on-line/off-line, and shared shutter status)
  - Data provision to higher level control systems (EPICS)
  - Common appearance within the two communities
  - Dual programmers
- **ACIS/PSS Differences:**
  - Due to geography and concurrent occupation, the ACIS includes testing and bypass functions controlled by key switches.
  - The PSS adheres to a more limited set of implementation rules and employs different vendor PLCs.

QUESTIONS?

Overview PSS Generation 1

Jon Hawkins

Agenda

- Scope
- PSS Generation I Overview – Design
- PSS Generation I Overview – Operations

Scope

- The scope of this discussion is primarily limited to our experiences using digital computer-based systems (e.g., programmable logic controllers PLC's) to implement the design of the **Personnel Safety System (PSS)** Generation I for beamlines at the Advanced Photon Source (APS) for the period 1996 to 2002.

- This qualitative presentation on **PSS Generation I** is intended as an historical and design reference point and as such is outside the charge to this review committee.

- By definition:
  - PSS Generation 1 => Initial plus evolved design at all existing beamlines except 4ID.
  - PSS Generation 2 => Test design at 4ID using lessons learned from PSS Gen. 1.
  - PSS Generation 3 => Design from lessons learned at 4ID PSS Gen 2.

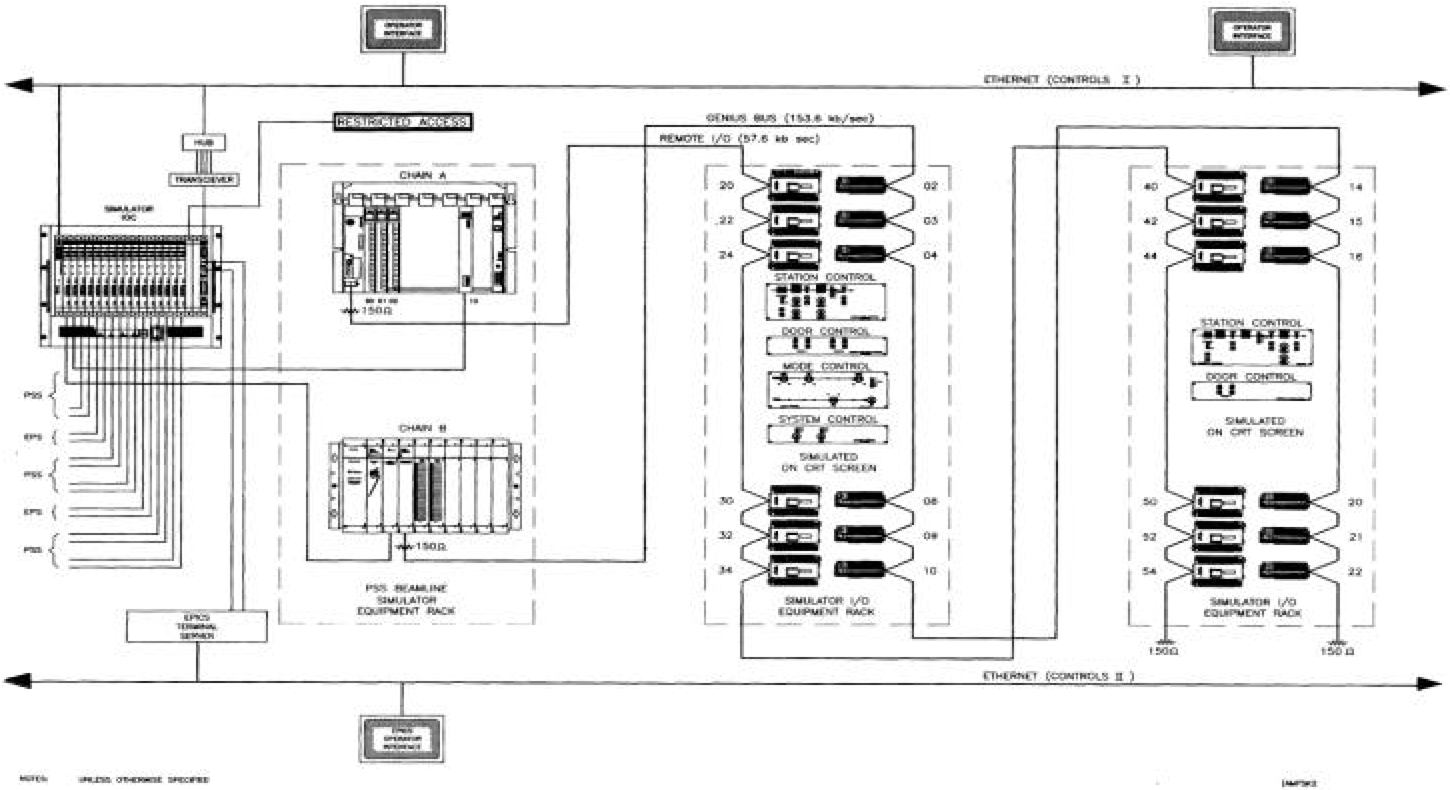
PSS Generation I: Overview - Design

- **Design Criteria &Guidance**
  - DOE ASO (420.2), SLAC-327, APS SAD, ANL ESH, etc.
  - Design & operational reviews (external & internal).

- **Design Requirements**
  - No single point of failure (redundancy).
  - Fail-Safe design.
  - Strict configuration controls (software & hardware).
  - Periodic functional testing (normal & off normal modes).
  - Personnel access control that protects from potential for prompt synchrotron radiation.
  - PSS has no direct measure for the presence of beam radiation.
  - Prompt beam radiation in all experimental considered lethal.

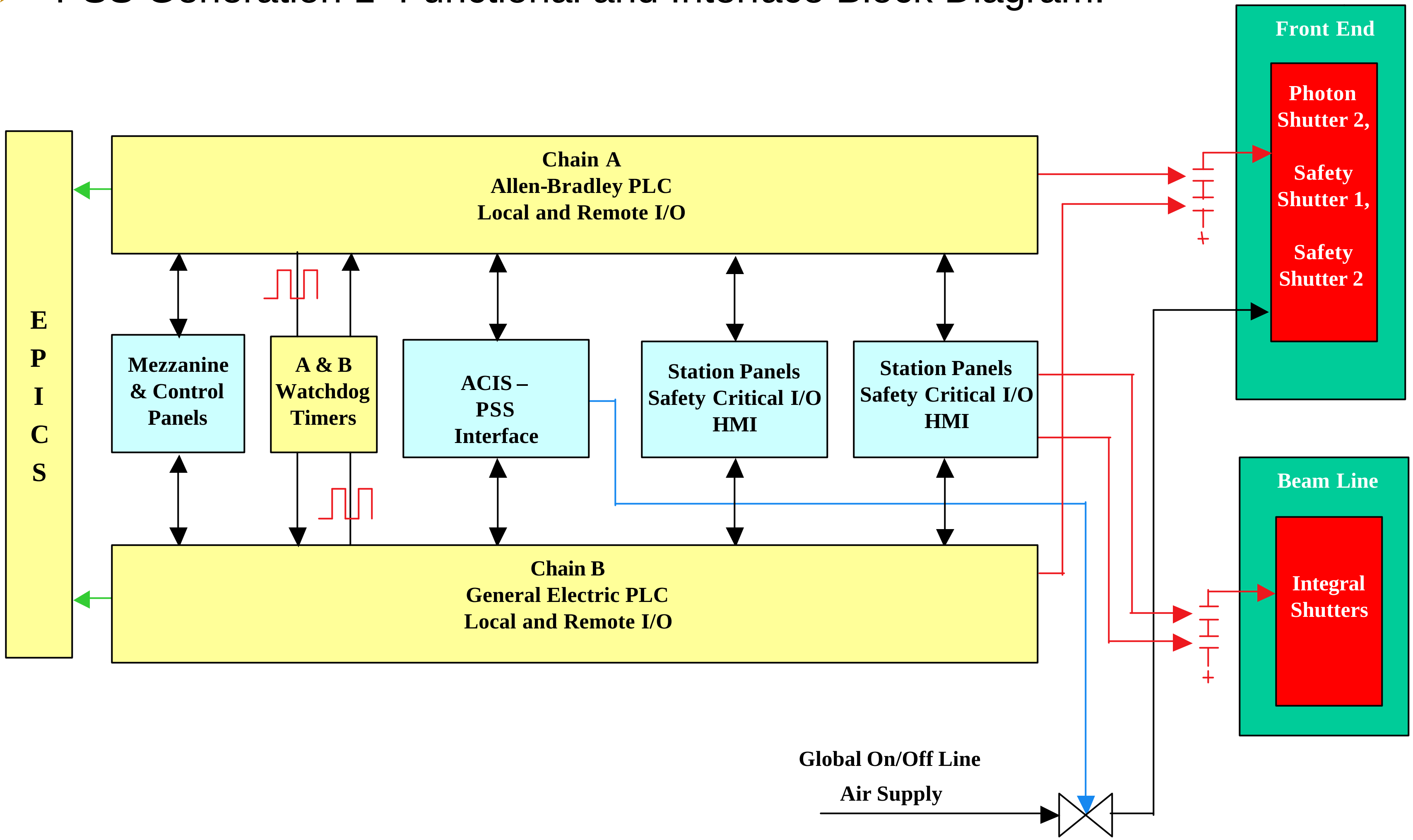
PSS Generation I: Overview - __Design__

- PSS Gen 1 schematic and layout.



PSS Generation I: Overview - __Design__

- PSS Generation 1 Functional and Interface Block Diagram.



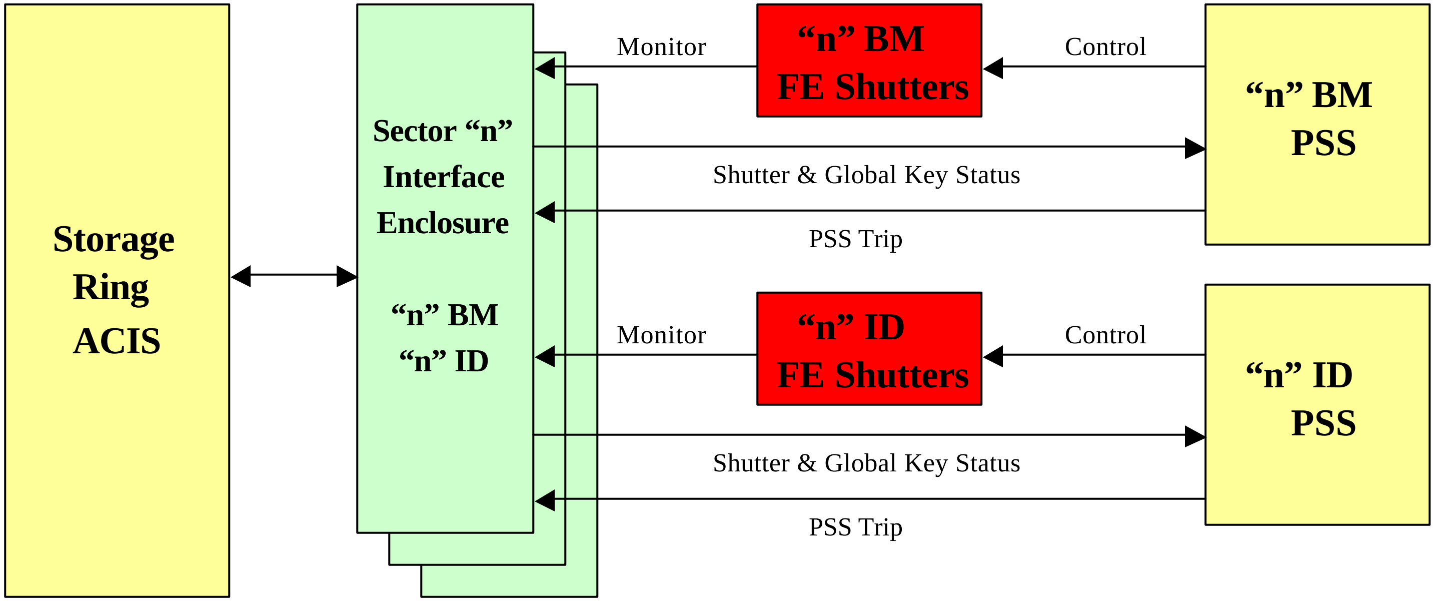
PSS Generation I: Overview - Design

- **Each PSS consists of two independent logic solving PLC chains (A&B)**
  - **Chain A** utilizes Allen-Bradley PLCs, programmed in ladder logic, **Chain B** General Electric PLCs, programmed in state logic.
  - Unique hard-wired addresses used for configuration control.
  - External watchdog timers added for additional reliability.

- **Common cause failures are addressed by**:
  - Using redundant, fail safe protection systems.
  - Different types of PLC's for each independent chain
    - *Value of vender diversity less on complex systems but recommended and implemented.*
  - Redundant door switches of different types (mechanical & magnetic).
  - Using different programmers and dissimilar software architectures to develop the software for each chain.

PSS Generation I: Overview - <u>Design</u>

- **PSS Interfaces**
  - Electrically Isolated (relay).
  - ACIS/PSS interface, few signals, **PSS permit**, **Global Off Line** function for testing PSS during storage ring operation, front end shutter closed switches shared.
  - FEEPS, BLEPS, DIW and RSI (Mezzanine or **front end (FE)** PSS**).**



PSS Generation I: Overview - Design

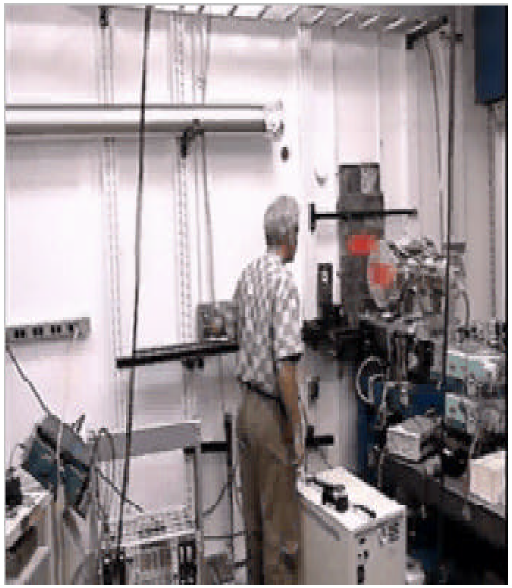
- **Protective Logic**
  - Simplified: “Doors” open means critical devices “closed”.
  - Outputs positive true logic.
  - Fault behavior: All PSS faults close all beamline shutters.
  - Chain A – **emergency shutdown (ESD)** function + command and control, faults.
  - Chain B – ESD, permit based (not faults =>EPICS).
  - Minimize diagnostics and embedded testing functions in code.
  - PSS code tested in “lab” before validated in the field (useful for trouble shooting and training).

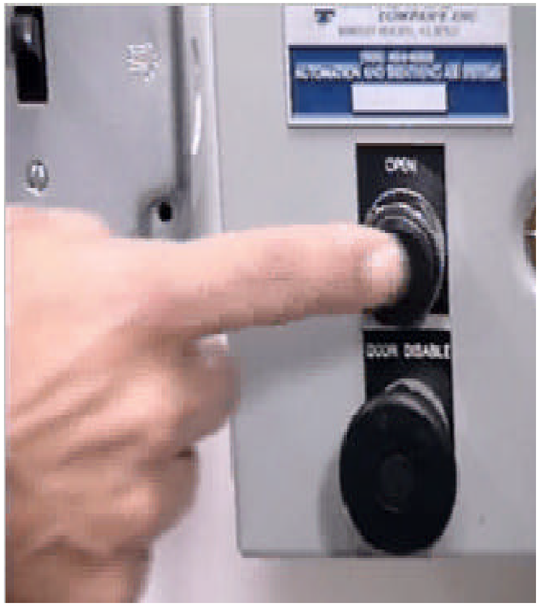
*PSS Generation I: Overview - **Design***

- PSS hardware components are located in **locked** cabinets**.**

PSS Generation I: Overview - Design

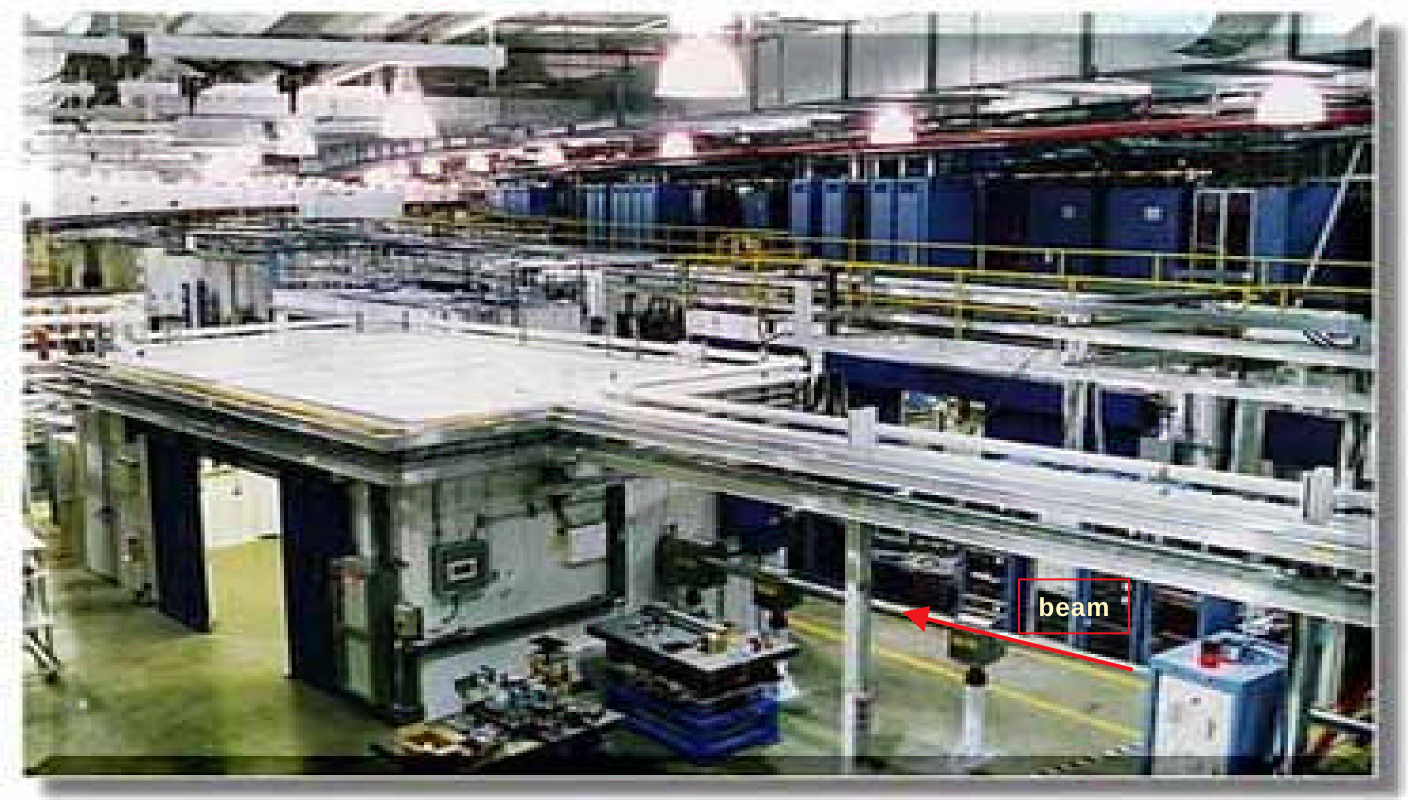
- The PSS includes emergency shut-off devices, status displays, enforced searches and emergency exit mechanisms.





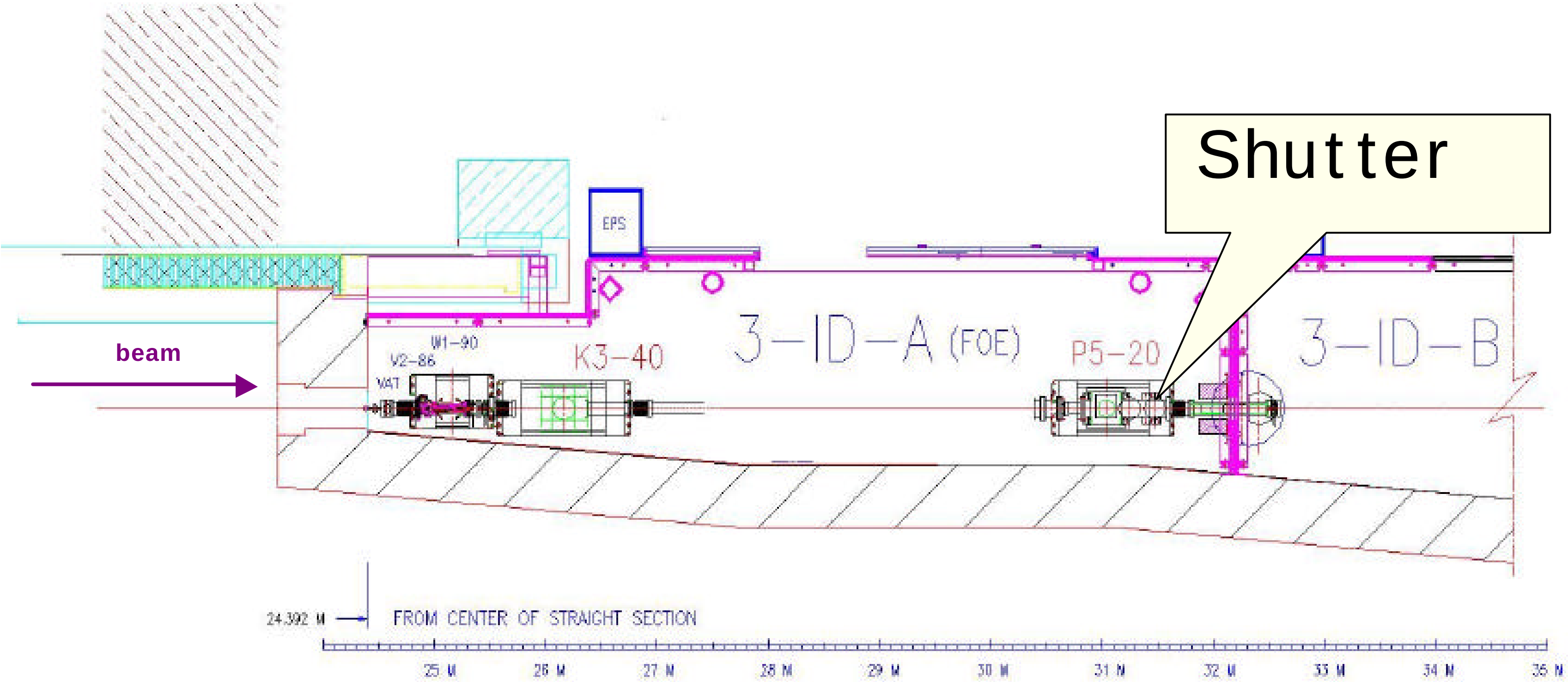
PSS Generation I: Overview - Design

- Typical beamline station.
- Complexity in beamline *operating modes*, canted undulator FE (2 beams =>more stations), frequency of user change requests and the phased commissioning of beamlines made the use of PLCs, the natural choice.
- All beamline PSS's are different.



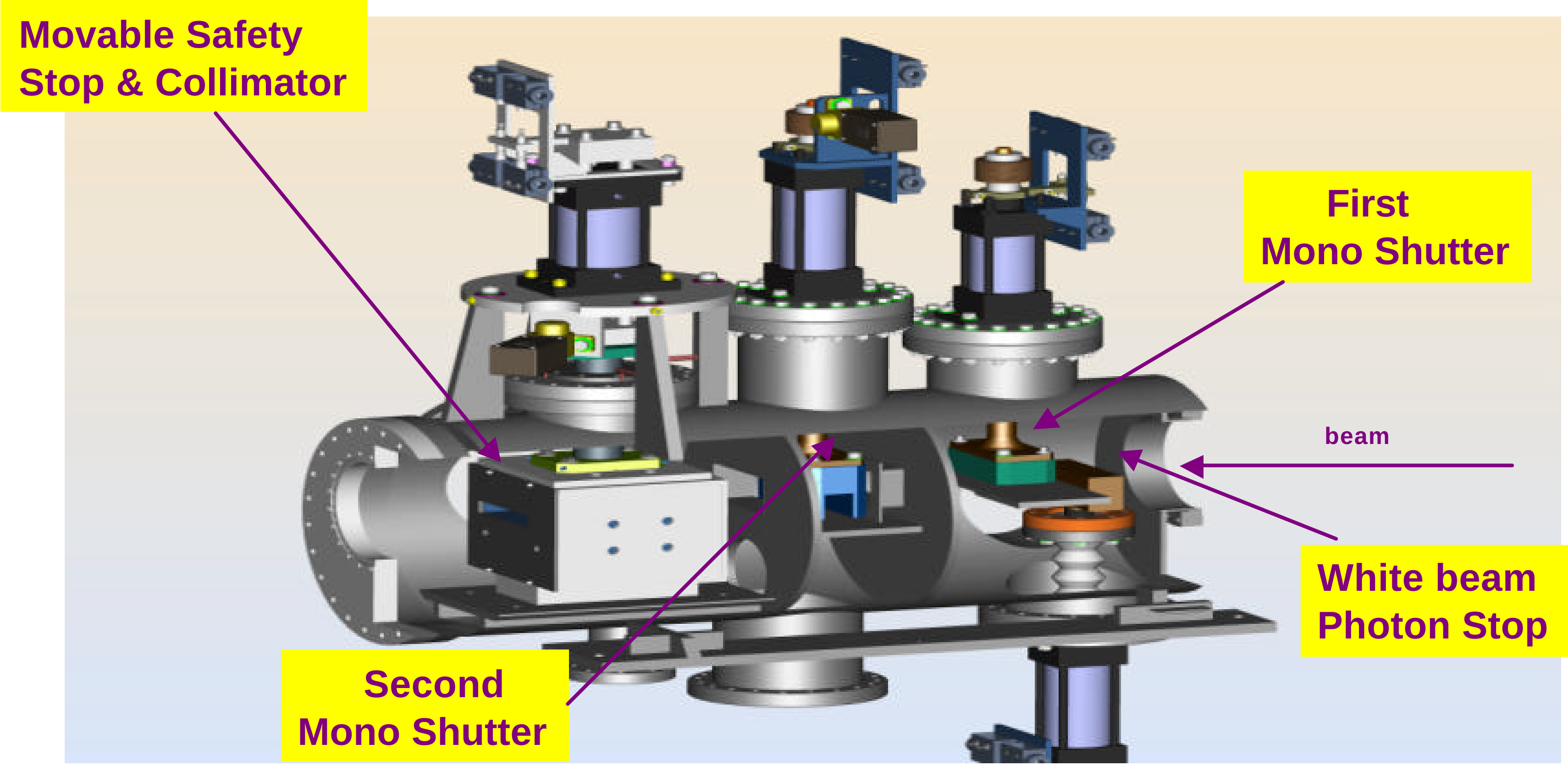
PSS Generation I: Overview - Design

- Typical Beamline Enclosure with Critical Device.
- Typical Insertion Device beam power density ~ 150 watts/sq mm
  - ID beam Total power ~ 5KW. => special **photon stop (PS)** design.
  - PS protects movable beam safety stops.



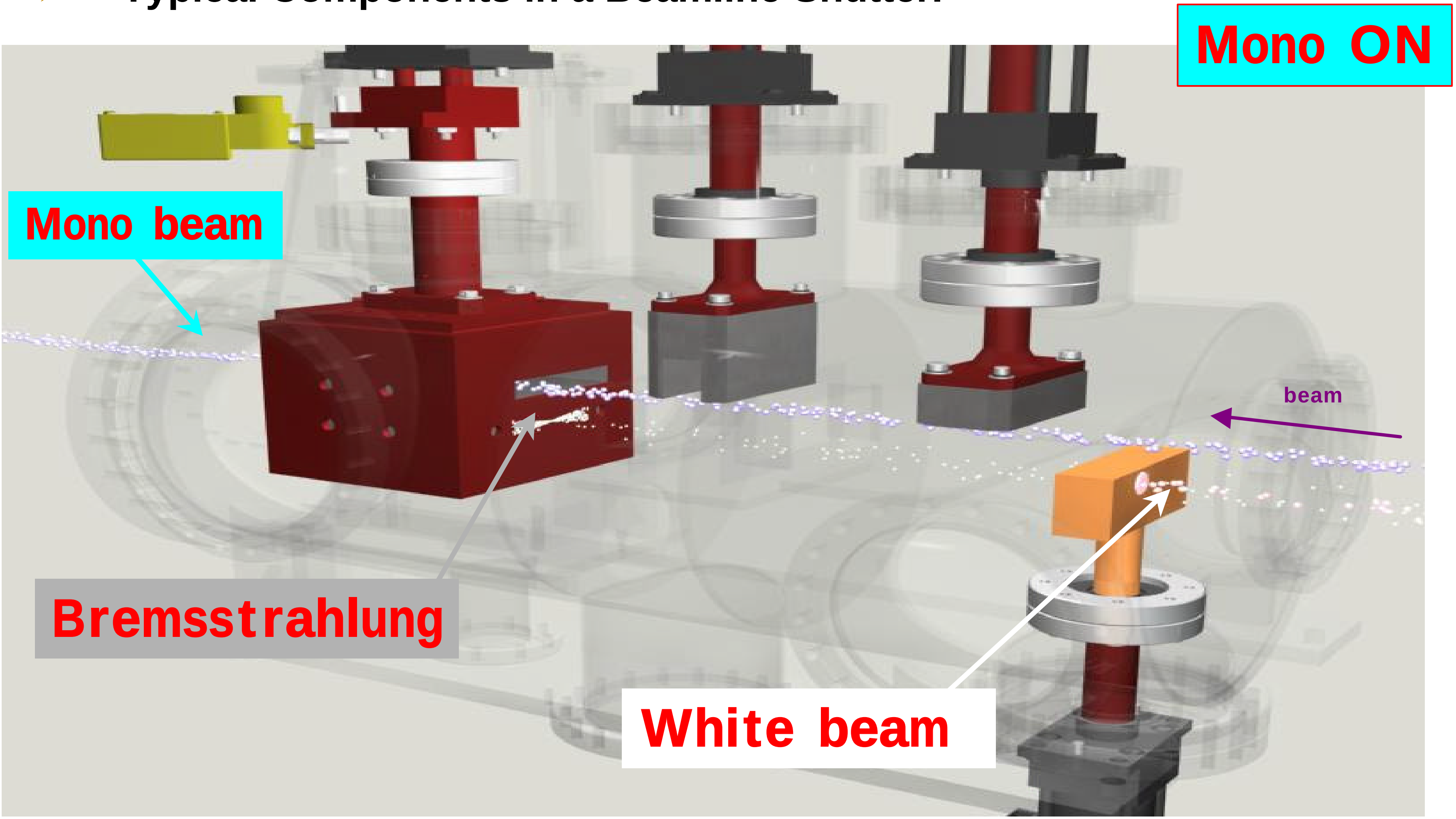
PSS Generation I: Overview - Design

- Typical Components in a Beamline Shutter.
- Typical photon beam types: white (synchrotron), monochromatic (narrow BW).
- Sequencing components to protect safety stops.



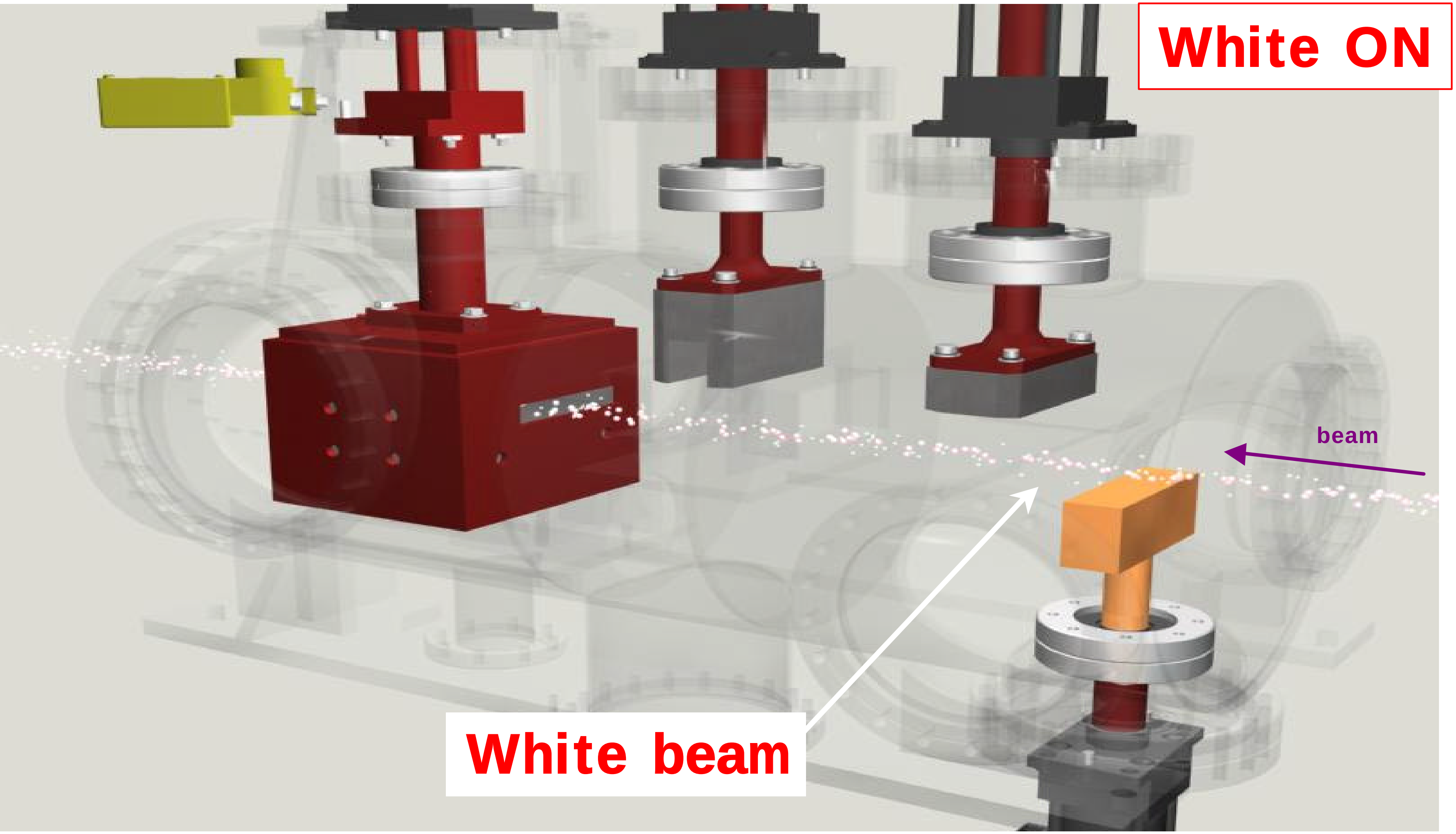
PSS Generation I: Overview - Design

- Typical Components in a Beamline Shutter.



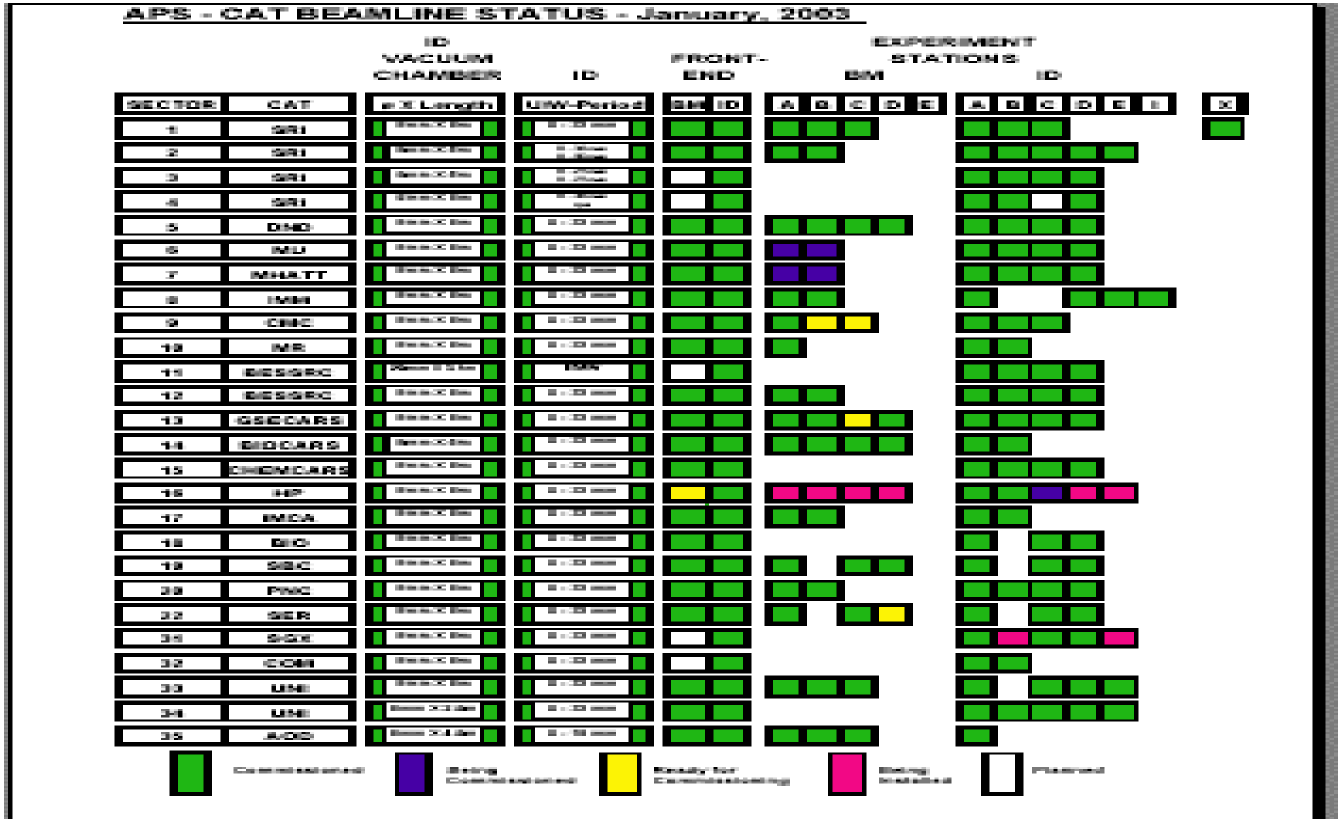
PSS Generation I: Overview - Design

- Typical Components in a Beamline Shutter.



PSS Generation I: Overview – Operations
(Managing Change)

- Currently 44 beamlines, 88 critical computer based systems, ~2500 signals abort SR.
- At or within SR availability budget.
- Over 95% of PSS-related User down time due to either shutter problems or station door operation not PSS operation (“wear items”, RE).



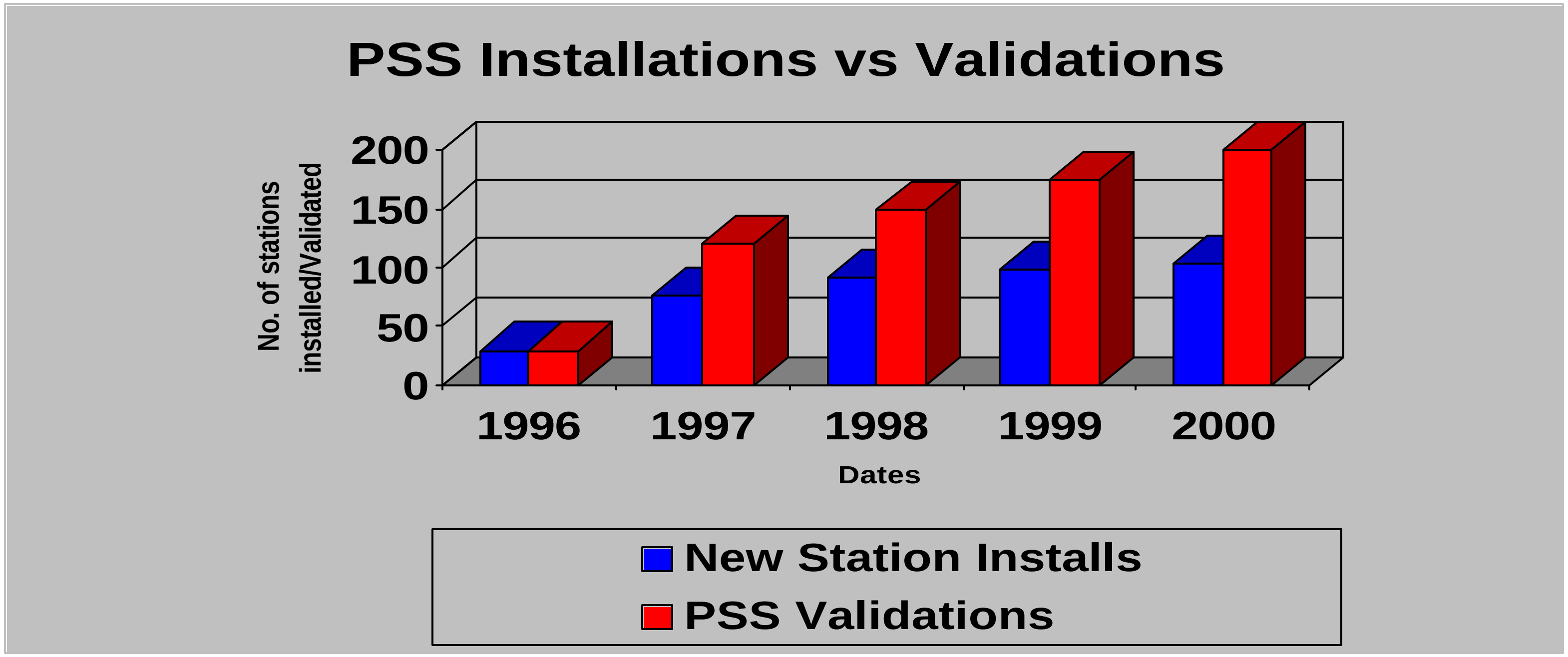
APS - CAT BEAMLINE STATUS - January, 2003

		ID VACUUM CHAMBER	ID	FRONT-END		EXPERIMENT STATIONS												
						BM					ID							
SECTOR	CAT	ø X Length	UW-Period	BM	ID	A	B	C	D	E	A	B	C	D	E	I		X
1	SRI	[illegible]	[illegible]	🟩	🟩	🟩	🟩	🟩			🟩	🟩	🟩					🟩
2	SRI	[illegible]	[illegible]	🟩	🟩	🟩	🟩				🟩	🟩	🟩	🟩	🟩			
3	SRI	[illegible]	[illegible]	⬜	🟩						🟩	🟩	🟩	🟩				
4	SRI	[illegible]	[illegible]	⬜	🟩						🟩	🟩	⬜	🟩				
5	DND	[illegible]	[illegible]	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	🟩				
6	MU	[illegible]	[illegible]	🟩	🟩	🟪	🟪				🟩	🟩	🟩	🟩				
7	MHATT	[illegible]	[illegible]	🟩	🟩	🟪	🟪				🟩	🟩	🟩	🟩				
8	IMM	[illegible]	[illegible]	🟩	🟩	🟩	🟩				🟩			🟩	🟩	🟩		
9	CMC	[illegible]	[illegible]	🟩	🟩	🟩	🟨	🟨			🟩	🟩	🟩					
10	MR	[illegible]	[illegible]	🟩	🟩	🟩					🟩	🟩						
11	BESSRC	[illegible]	[illegible]	⬜	🟩						🟩	🟩	🟩	🟩				
12	BESSRC	[illegible]	[illegible]	🟩	🟩	🟩	🟩				🟩	🟩	🟩	🟩				
13	GSECARS	[illegible]	[illegible]	🟩	🟩	🟩	🟩	🟨	🟩		🟩	🟩	🟩	🟩				
14	BIOCARS	[illegible]	[illegible]	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩						
15	CHEMCARS	[illegible]	[illegible]	🟩	🟩						🟩	🟩	🟩	🟩				
16	HP	[illegible]	[illegible]	🟨	🟩	🟥	🟥	🟥	🟥		🟩	🟩	🟪	🟥	🟥			
17	IMCA	[illegible]	[illegible]	🟩	🟩	🟩	🟩				🟩	🟩						
18	BIO	[illegible]	[illegible]	🟩	🟩						🟩		🟩	🟩				
19	SBC	[illegible]	[illegible]	🟩	🟩	🟩		🟩	🟩		🟩		🟩	🟩				
20	PNC	[illegible]	[illegible]	🟩	🟩	🟩	🟩				🟩	🟩	🟩	🟩				
22	SER	[illegible]	[illegible]	🟩	🟩	🟩		🟩	🟨		🟩		🟩	🟩				
31	SGX	[illegible]	[illegible]	⬜	🟩						🟩	🟥	🟩	🟩	🟥			
32	COM	[illegible]	[illegible]	⬜	🟩						🟩	🟩						
33	UNI	[illegible]	[illegible]	🟩	🟩	🟩	🟩	🟩			🟩		🟩	🟩	🟩			
34	UNI	[illegible]	[illegible]	🟩	🟩						🟩	🟩	🟩	🟩	🟩			
35	ADO	[illegible]	[illegible]	🟩	🟩	🟩	🟩	🟩			🟩							

🟩 Commissioned 🟪 Being Commissioned 🟨 Ready for Commissioning 🟥 Being Installed ⬜ Planned

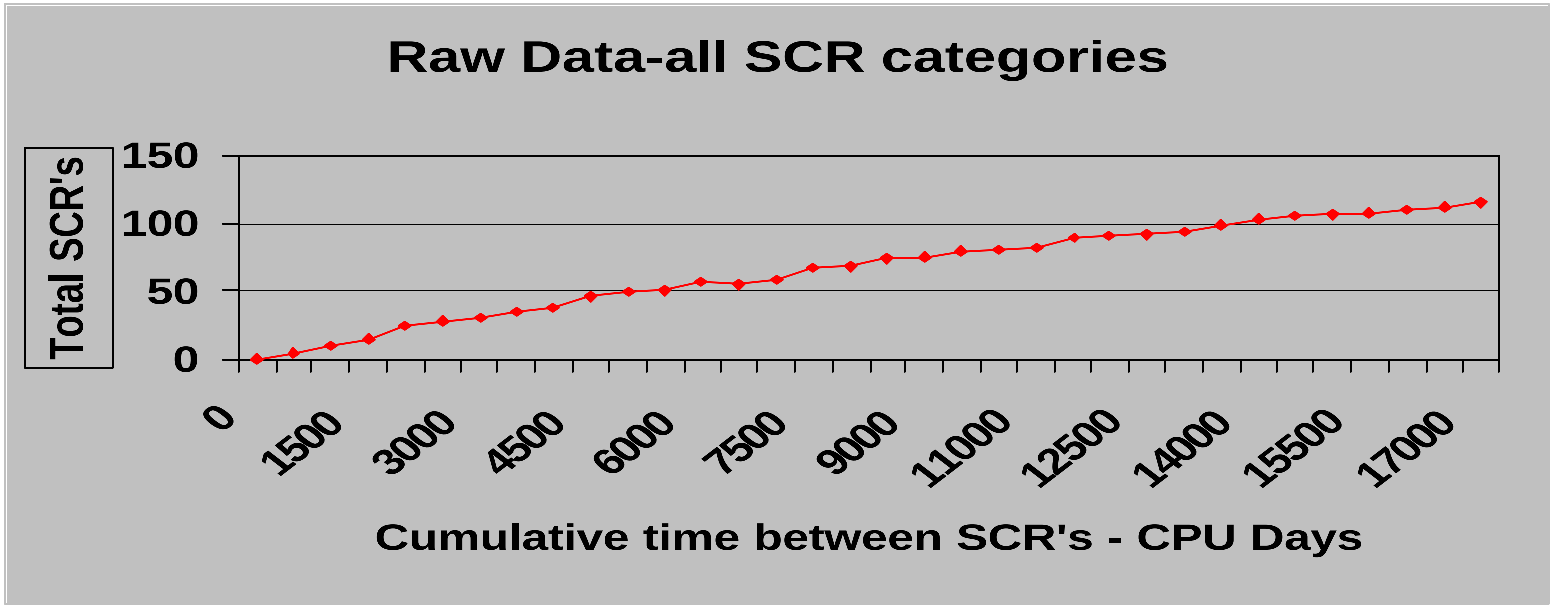
PSS Generation I: Overview – Operations
(Managing Change)

- Performed PSS validations on over 700 stations during the same 64-month period.
- PSS validation schedule >85% on time, to the day over six months.



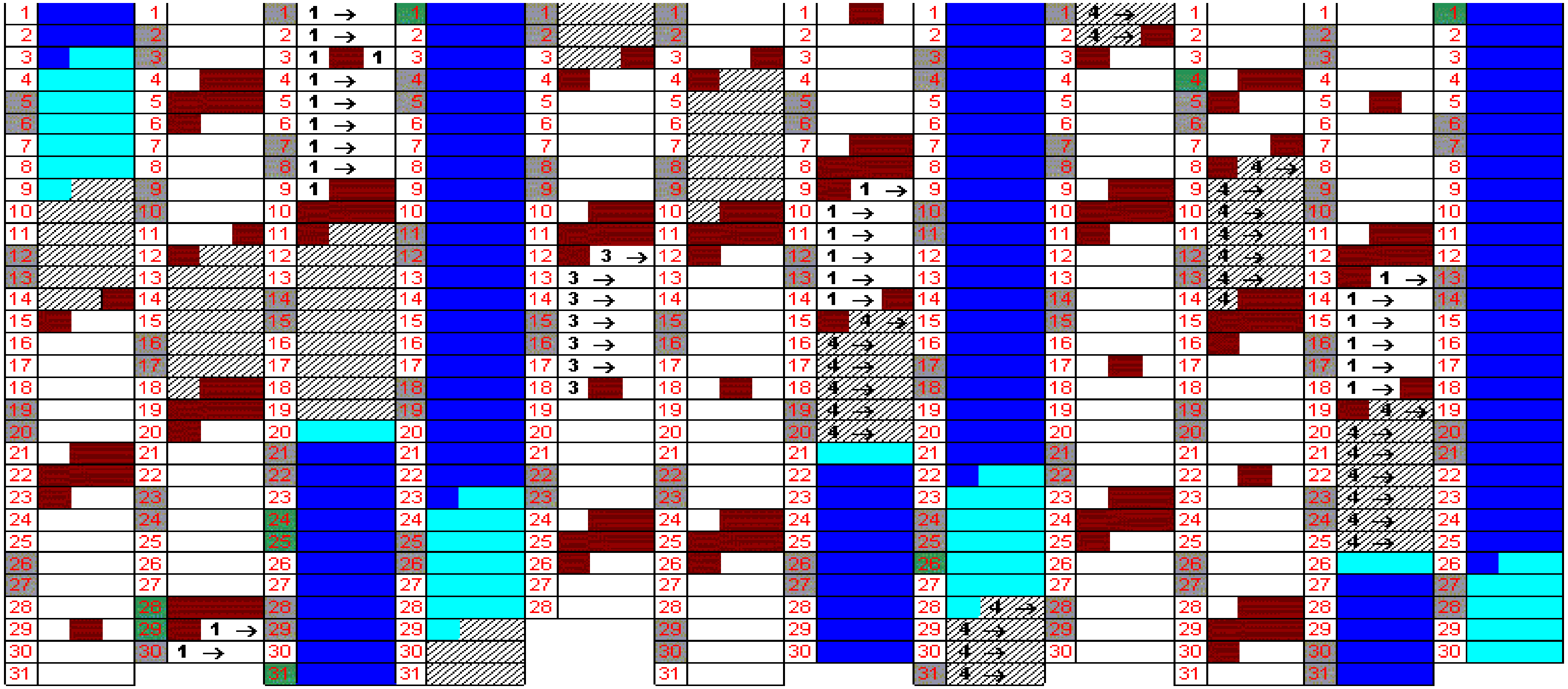
PSS Generation I: Overview – Operations
(Managing Change)

- PSS activities plus User operational change requests resulted in over 200 reviewed and approved software change requests (SCRs) during the same 64-month period. Only 5-10% ESD code.
- SCR's included phased commissioning of beamlines plus growth of beamline/user needs (e.g. S&S zones, shutters changed/moved, search times change, etc. => one per beamline per ~ 18 months).
- No loss of PSS ESD protection during this period.



PSS Generation I: Overview – Operations (Lessons Learned)

- Change to annual validations of APS Personnel Safety Systems.
- Reasons: increasing number of beamlines and 3-shutdown schedule.
- Justification: Favorable Operating Reliability, Conservative PLC Reliability estimates.



PSS Generation I: Overview – Operations
(Key Challenges)

- Evidence strongly suggests that APS Users will continue to need semi-custom and dynamic PSS operational profiles (i.e., HMI) Canted Undulator Beamlines (I/O space limited). Few changes to ESD.

- Improve testing methods => less intrusive test methods.

- Improve PSS trip recovery and MTBF via diagnostics, Develop Beamline availability/usage measure.

- Reliability – future preventative maintenance issues with loss of vender support.

Overview PSS Generation 1

QUESTIONS?

Statement of Work
Migration from Generation-1 to Generation-3
and
Feature comparison of Generation-1 to Generation-2 and Generation-3

Roy Emerson

Statement of Work – Our Goals

- **Our Goals**
- **Operations and Safety**
  - The PSS system must meet Safety, Reliability and Operational needs of the APS and users.
  - We will first talk about some but not all of the ways we meet the safety requirements of DOE, ES&H, APS and the User community.
  - Second we will discuss how we plan to achieve reliability.
  - Last we will explain the operational aspects of the PSS.

Operational and Safety Considerations

- **Meet the safety and operational needs of the APS beamlines in a cost-effective manner.**
- **Meet the operational and reliability needs of APS machine and beamline operations.**
- **System should be designed with the intention of building this version for five years and supporting it for ten years.**
- **Flexibility**
  - The system shall be sufficiently flexible to accommodate all known and anticipated beamline configurations.
- **Expandable**
  - The system shall be sufficiently expandable to accommodate all known and anticipated beamline configurations.

System Capabilities

- **Reliability**
  - The system shall be reliable to support the reliability goals of the accelerator and beamlines.
- **Availability**
  - The system shall be easily serviceable to support the availability goals of the accelerator and beamlines.
- **System should not be unnecessarily complicated to operate or support, so as to minimize the possibility of human error during operation, validations, and servicing.**

- **System should not be unnecessarily complicated to operate or support, so as to minimize the possibility of human error during operation, validations, and servicing.**

- **As much as reasonable, system should provide self-diagnostics for troubleshooting and fault information.**

Validation Improvement

- **Non-Invasive Validations**
  - Support will be provided for non-invasive PSS validations.
  - Removal and re-connection of existing field wiring should be minimized when performing PSS validations. Connection of additional devices (e.g. to dedicated connectors) is acceptable. Removal of field wiring to make such connections (e.g. as done now for front-end simulator) is not acceptable.
  - Monitoring of PLC status required for PSS validations should not require direct access to the PLC code, as is done now. Hookup of a separate computer is acceptable provided it does not make or facilitate changes in PLC code or checksums.
  - Downloading of PSS code should be streamlined to minimize the possibility of errors.

Validation Improvement

- **Time Reduction**
  - System design should facilitate reducing PSS validation times.
- **Validation Quality**
  - There must be no compromise in the system coverage of the validation.
- **Self Test Capabilities**
  - As much as reasonable, system should provide self-test capabilities, e.g. to perform a partial PSS validation with a button push.
- **All information that could be valuable for operations support shall be provided to EPICS. This includes event capture, trending, and problem diagnosis.**

Backward Compatibility

- It should be possible to retrofit key benefits of Generation-3 to existing Generation-1 and Generation-2 systems. At a minimum, it should be possible to eliminate needs to remove field wiring when hooking up validation equipment. It is also desirable to provide support for self-test and automated PSS validations, and for other benefits as appropriate.

Statement of Work

QUESTIONS?

Migration – Why Change

Migration from Gen-1 to Gen-3, justification for Gen-3 development

Roy Emerson

Migration – Why Change

- **Justification for Generation-3 development**
  - Machine operating schedules (5000 Hours of delivered beam).
  - Three shutdowns for all PSS work requiring no beam in Ring.
  - 45 Beamlines ~ 135 Stations.
  - Manpower requirements for maintenance and validations.
  - Goal is to reduce validation time to 1 day.
  - Canted undulator beam lines
    - *Doubles the beam from the ring.*
    - *More stations in each line.*
    - *More complex operating configurations.*
  - Eliminate Disconnect and reconnect of field devices for testing.
  - Eliminate point to point wiring replace with circuit boards.

Migration – Why Change

- **Justification for Generation-3 development (cont.)**
  - Improve system reliability replacing electro-mechanical watchdog interface with optically isolated solid state devices.
  - Version-1 PSS cannot support some of the proposed upcoming beam line designs.
  - Allen-Bradley has provided notification they are discontinuing production of several of the Input/output modules and VME modules used in our current design.
  - GE has provided notification they are replacing their State-logic processors with a redesigned version that will require changing both the hardware and the programming software to allow its use in our PSS systems.
  - Significant hardware technology improvements have been released by Allen-Bradley, GE and other vendors at a lower cost since the original design.

Migration – Why Change

- **Justification for Generation-3 development (cont.)**
  - We have had many requests to change the user interface. This has been difficult using the hardwired user interface. We have moved to Soft panel Touch Screens to solve this problem. Many benefits – ease of change, added diagnostics, no revalidation, easier to trouble shoot at a non-technical level.
  - Separation of Command and Control from the Emergency Shut Down part of the system provides many benefits. ESD code is simplified resulting in a more robust easier to validate system. Less code equals less to test, less potential errors, less complexity making it easier to understand.
  - Due to an ever increasing human resources requirement for V&V, there is significant motivation to reduce V&V time while at the same time increasing accuracy through automation.

Migration – Why Change

- **Justification for Generation-3 development (cont.)**
  - Lessons Learned from Generation-1 and Generation-2 point to many improvements that should be made in the system
    - *Examples:*
      - More modular design easier easier to accommodate users needs and unforeseen future changes.
      - Non-invasive interface for testing.
      - Touch Screen display of diagnostic information – a huge improvement over two blinking lights.
      - Infrastructure for automated validations allowing the system to perform the validations to reduce the human error due to inconsistent testing.
      - Full integration with EPICS allowing both status and remote control.

Migration – Why Change

- **Summary**
  - There are a large number of reasons to move to a third generation PSS system.
  - A number of these reasons are sufficient by themselves.
  - Taken together the reasons identified provide a very compelling justification for a third generation PSS system.

Migration – Why Change

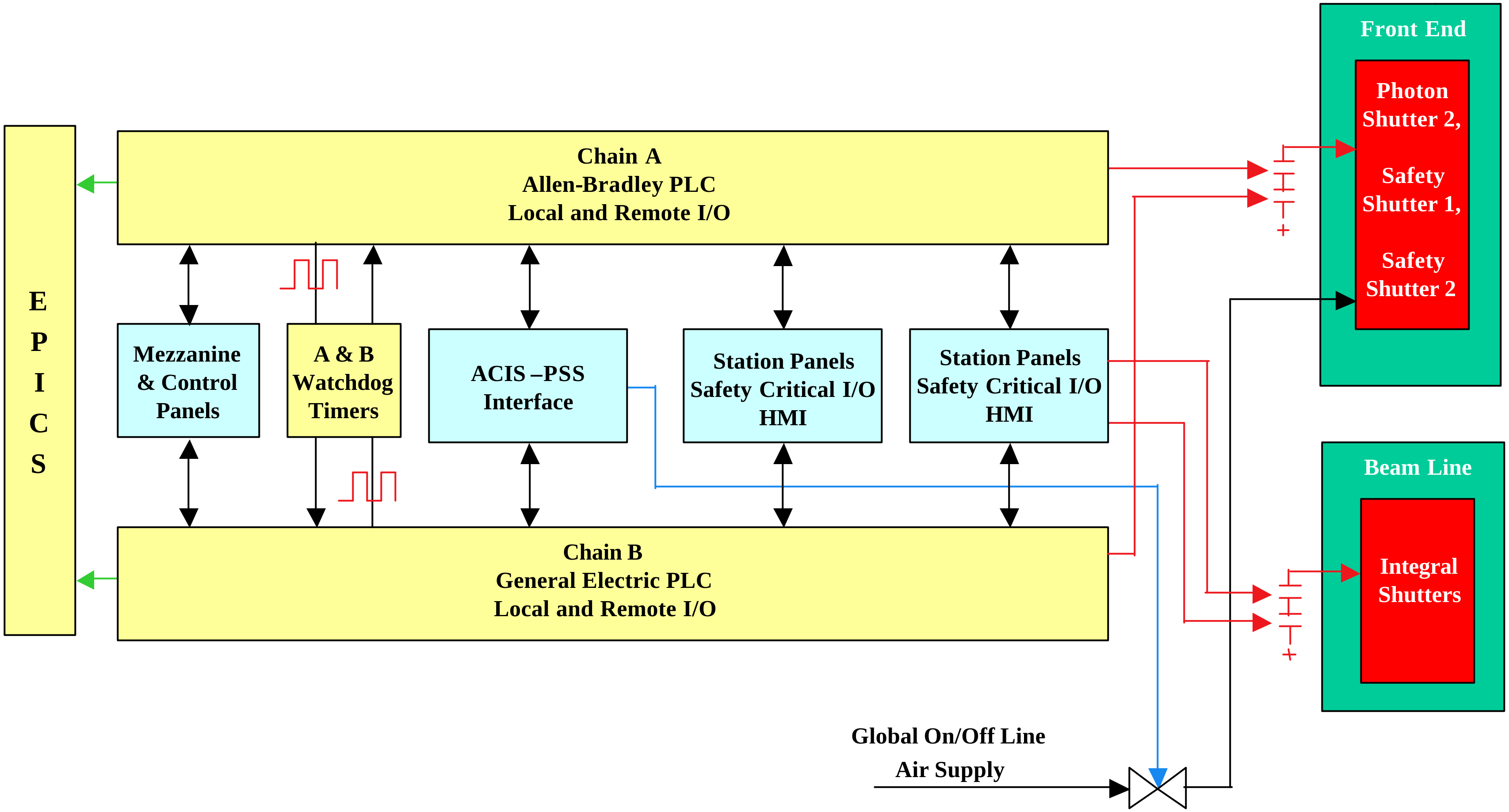
QUESTIONS?

A Feature comparison of Generation-1 / Generation-2 / Generation-3 PSS

Roy Emerson

The Features of The PSS

Generation-1 PSS



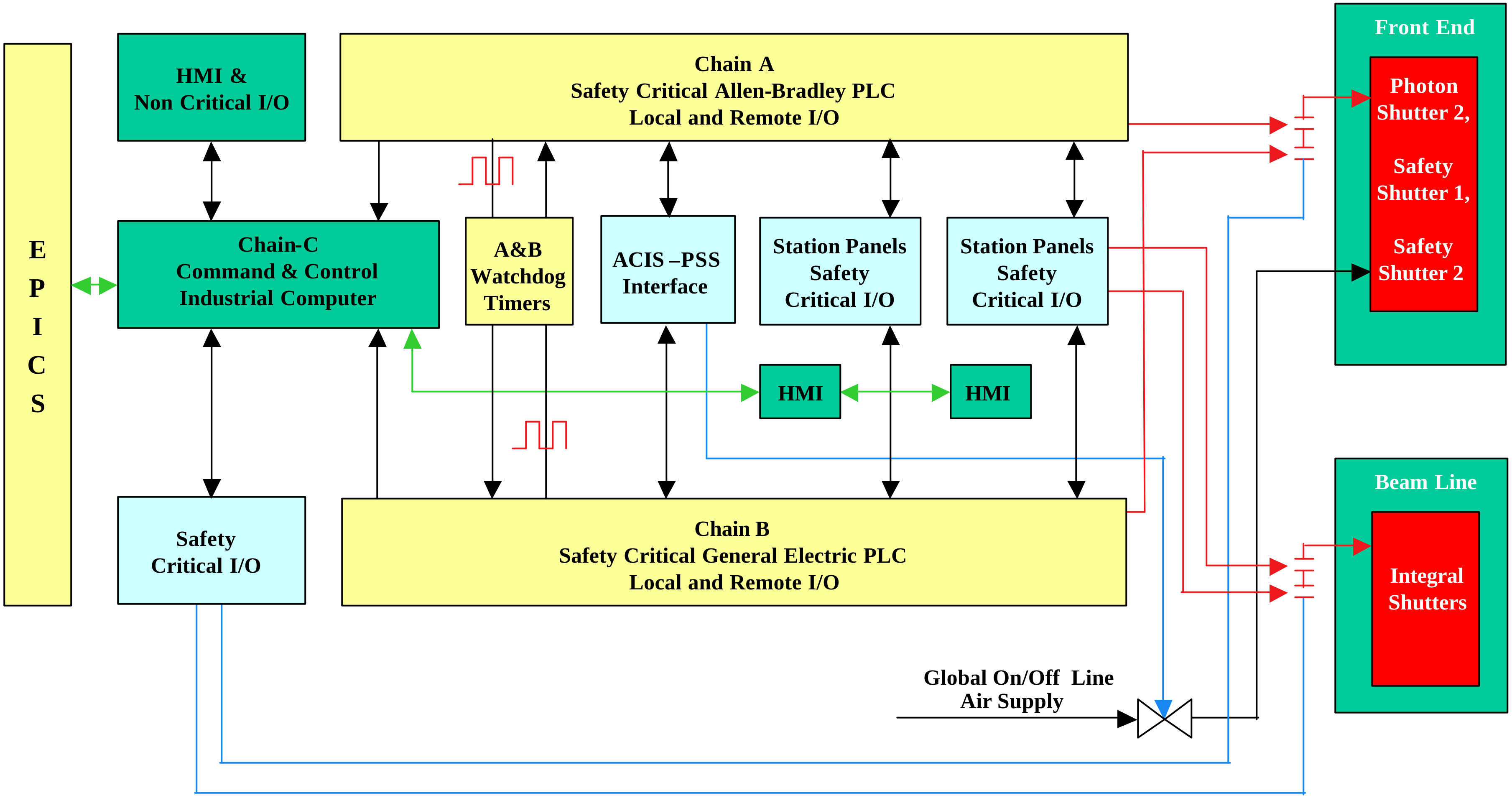
The Features of The PSS

Generation-2
A brief introduction

- **Generation-2 represents fundamental shift is how we build a safety system**
  - The “PSS Safety System” was originally designed using two PLC systems to perform all of the functions needed
    - *Emergency Shut Down.*
    - *Administrative Procedure Enforcement.*
    - *System Diagnostics.*
    - *Provide system status to the operator.*
    - *Act upon operator input.*
    - *Etc.*
  - The largest compliment of code and I/O is devoted to providing status and acting on operator input (the operator interface).
  - Generation-2 relocated the operator interface to a third system.

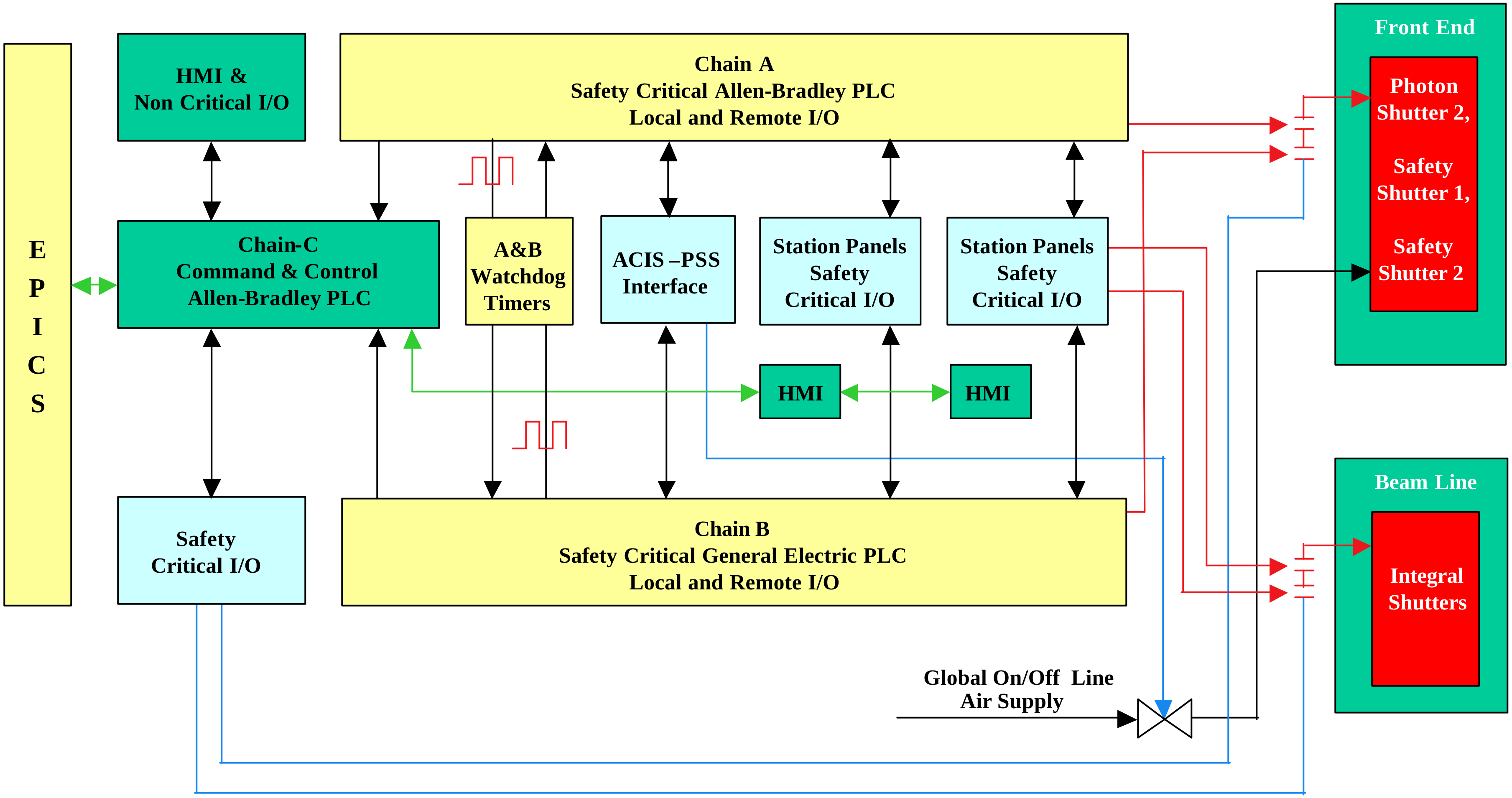
The Features of The PSS

Generation-2 PSS



The Features of The PSS

Generation-3 PSS


E P I C S
HMI & Non Critical I/O
Chain A Safety Critical Allen-Bradley PLC Local and Remote I/O
Front End
Photon Shutter 2,
Safety Shutter 1,
Safety Shutter 2
Chain-C Command & Control Allen-Bradley PLC
A&B Watchdog Timers
ACIS –PSS Interface
Station Panels Safety Critical I/O
Station Panels Safety Critical I/O
HMI
HMI
Beam Line
Integral Shutters
Safety Critical I/O
Chain B Safety Critical General Electric PLC Local and Remote I/O
Global On/Off Line Air Supply

The Features of The PSS

Generation-1 Function Partitioning

Chain A

ESD

- Monitor Global Off-line Shutter Disable
- Monitor Search and Secure Status
  - Monitor Crash Button
  - Monitor Door Closed
- Monitor Shutter Operation
  - Monitor Air Pressure
  - Monitor DIW
- Issue and Remove Storage Ring Permit
- Monitor Chain-B Watchdog

User Interface

- Automatic Door Operation
- Manual Door Locks
- Control Panel Arbitration
- Shutter Operation
- Operator Tactile Feedback

Administrative Control and Permits

- Enforce Search and Secure
- ACIS Permit Enforcement
- APS Enable Key Enforcement
- User Enable Key Enforcement
- FE-EPS Permit Enforcement
- BL-EPS Permit Enforcement
- Mode Shutter Control and Monitoring
- Send Mode Shutter Status to Chain-B & BL-EPS
- Send Search Status to Chain-B
- Fault Reset

Status and Display

- Shutter Status Display
- Permit Status Display
- Online Status Display
- User and APS Enable Display
- Door Status Display
- Status to EPICS
- Fault Display (LED)

Chain B

ESD

- Monitor Global Off-line Shutter Disable
- Monitor Search and Secure Status
  - Monitor Crash Button
  - Monitor Door Closed
- Monitor Air Pressure
  - Monitor DIW
  - Issue Storage Ring Permit
- Issue Shutter Permits
- Monitor Chain-A Watchdog
- Permit removal NOT latched

Administrative Control

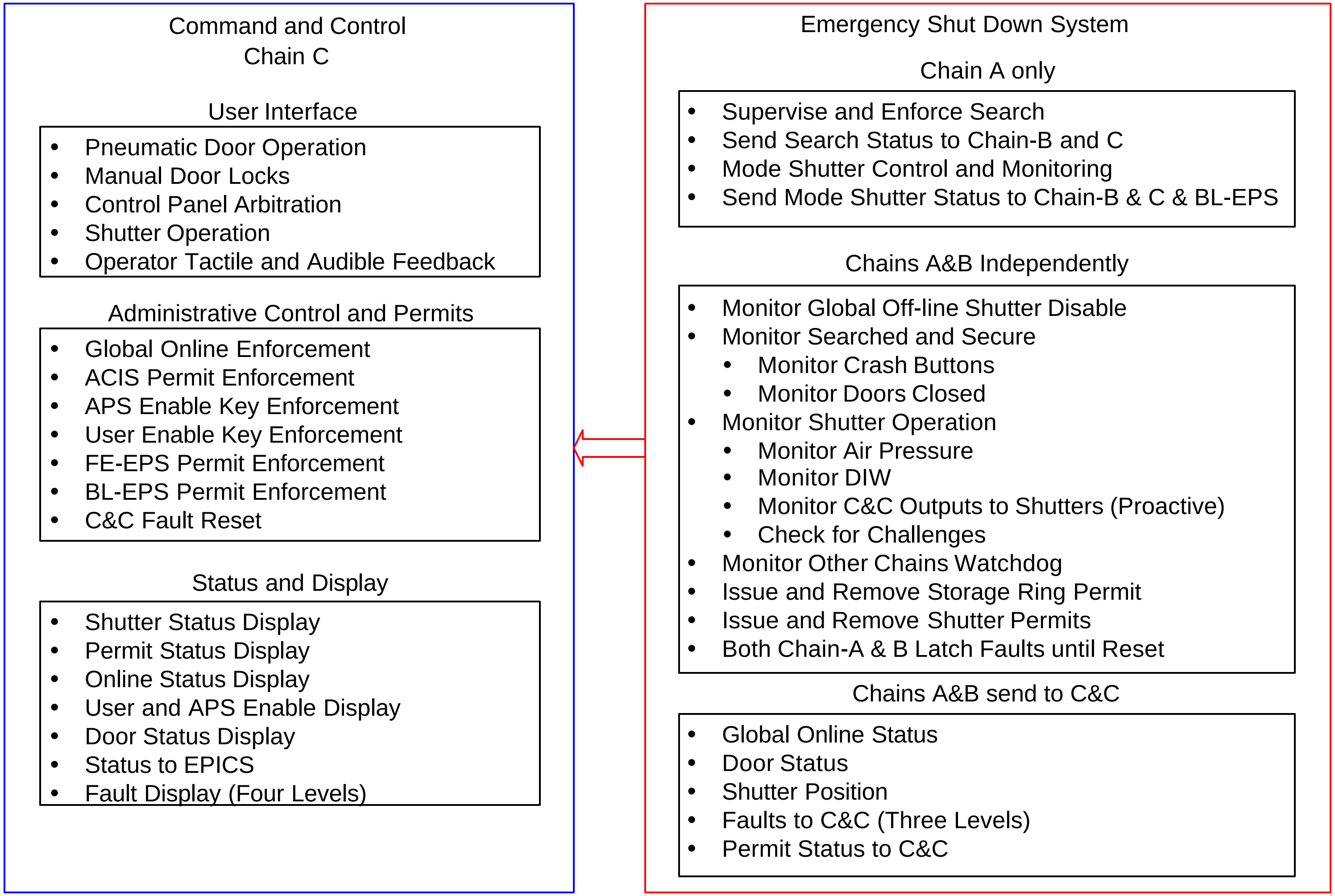
- ACIS Permit Enforcement
- APS Enable Key Enforcement
- User Enable Key Enforcement
- FE-EPS Permit Enforcement
- BL-EPS Permit Enforcement

Status and Display

- Shutter Status Display
- Permit Status Display
- Online Status Display
- User and APS Enable Display
- Door Status Display
- Status to EPICS
- NO Latched User Fault Data
- Shutter Permit Status to Chain-A

The Features of The PSS

Generation-2 Function Partitioning



Command and Control
Chain C

User Interface

- Pneumatic Door Operation
- Manual Door Locks
- Control Panel Arbitration
- Shutter Operation
- Operator Tactile and Audible Feedback

Administrative Control and Permits

- Global Online Enforcement
- ACIS Permit Enforcement
- APS Enable Key Enforcement
- User Enable Key Enforcement
- FE-EPS Permit Enforcement
- BL-EPS Permit Enforcement
- C&C Fault Reset

Status and Display

- Shutter Status Display
- Permit Status Display
- Online Status Display
- User and APS Enable Display
- Door Status Display
- Status to EPICS
- Fault Display (Four Levels)

Emergency Shut Down System

Chain A only

- Supervise and Enforce Search
- Send Search Status to Chain-B and C
- Mode Shutter Control and Monitoring
- Send Mode Shutter Status to Chain-B & C & BL-EPS

Chains A&B Independently

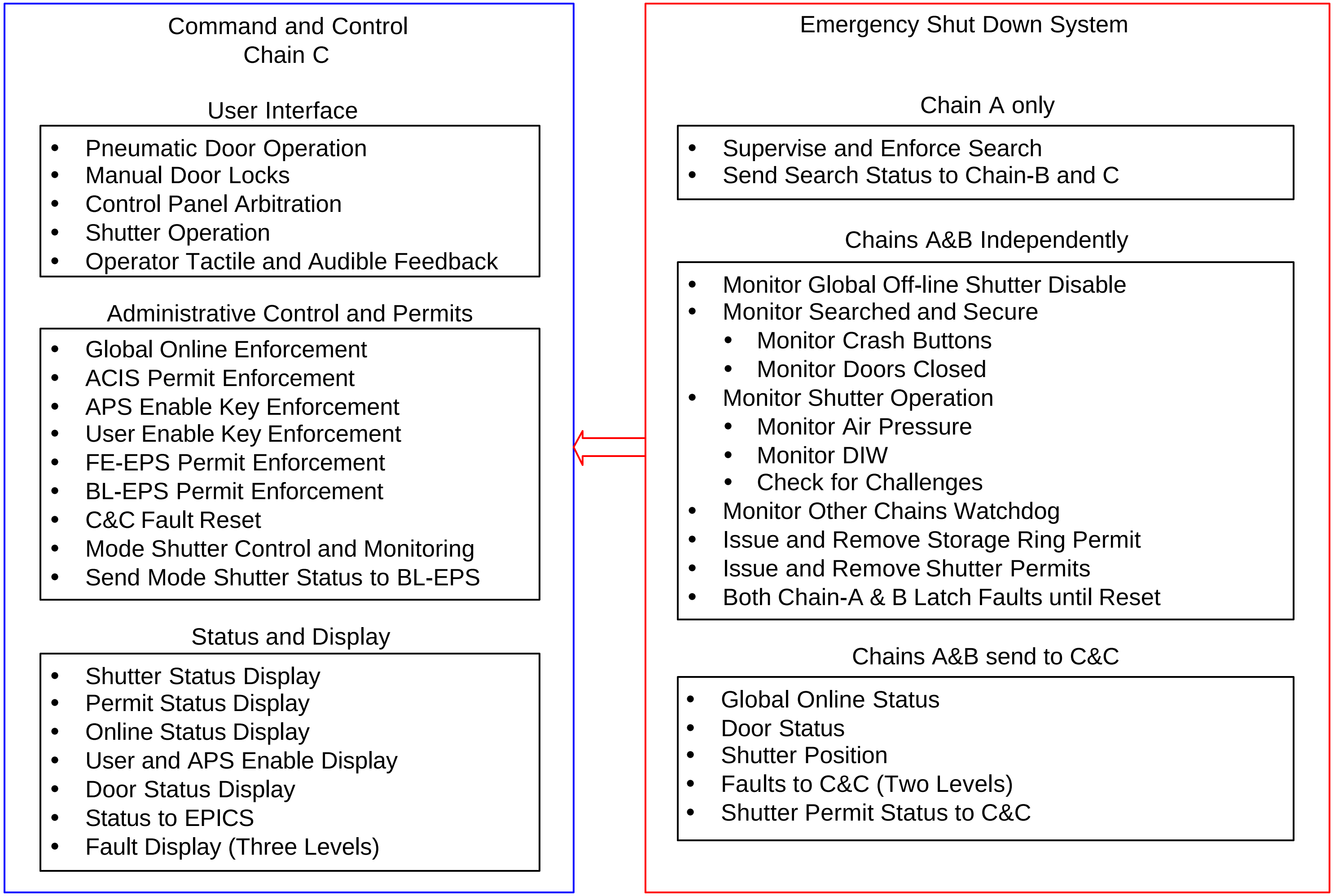
- Monitor Global Off-line Shutter Disable
- Monitor Searched and Secure
  - Monitor Crash Buttons
  - Monitor Doors Closed
- Monitor Shutter Operation
  - Monitor Air Pressure
  - Monitor DIW
  - Monitor C&C Outputs to Shutters (Proactive)
  - Check for Challenges
- Monitor Other Chains Watchdog
- Issue and Remove Storage Ring Permit
- Issue and Remove Shutter Permits
- Both Chain-A & B Latch Faults until Reset

Chains A&B send to C&C

- Global Online Status
- Door Status
- Shutter Position
- Faults to C&C (Three Levels)
- Permit Status to C&C

The Features of The PSS

Generation-3 Function Partitioning



Command and Control
Chain C

User Interface

- Pneumatic Door Operation
- Manual Door Locks
- Control Panel Arbitration
- Shutter Operation
- Operator Tactile and Audible Feedback

Administrative Control and Permits

- Global Online Enforcement
- ACIS Permit Enforcement
- APS Enable Key Enforcement
- User Enable Key Enforcement
- FE-EPS Permit Enforcement
- BL-EPS Permit Enforcement
- C&C Fault Reset
- Mode Shutter Control and Monitoring
- Send Mode Shutter Status to BL-EPS

Status and Display

- Shutter Status Display
- Permit Status Display
- Online Status Display
- User and APS Enable Display
- Door Status Display
- Status to EPICS
- Fault Display (Three Levels)

Emergency Shut Down System

Chain A only

- Supervise and Enforce Search
- Send Search Status to Chain-B and C

Chains A&B Independently

- Monitor Global Off-line Shutter Disable
- Monitor Searched and Secure
  - Monitor Crash Buttons
  - Monitor Doors Closed
- Monitor Shutter Operation
  - Monitor Air Pressure
  - Monitor DIW
  - Check for Challenges
- Monitor Other Chains Watchdog
- Issue and Remove Storage Ring Permit
- Issue and Remove Shutter Permits
- Both Chain-A & B Latch Faults until Reset

Chains A&B send to C&C

- Global Online Status
- Door Status
- Shutter Position
- Faults to C&C (Two Levels)
- Shutter Permit Status to C&C

A Feature Comparison

PSS Features	Generation-1	Generation-2	Generation-3
Hardware			
Fail Safe Design	Yes	Yes	Yes
Command and Control Location	Chain-A	Chain-C	Chain-C
Emergency Shut Down	Chain-A & B	Chain-A & B	Chain-A & B
User Interface Hardwired	Yes	Minimal	Minimal
User Interface Soft Panel	No	Yes	Yes
Point to Point Wiring	Yes	Yes	No
Circuit Boards	No	No	Yes
Molded Plug-in Cables	No	No	Yes
Separate Power for Locks and Strobes	Update in Progress	Yes	Yes
Grounded System	No	Yes	Yes
Hardware Remote Shutter Operation	Yes	No	No
Expanded Equipment Capability	Limited (Ex 5 Doors)	Better (Ex 6 Doors)	Known + 10%
Modular PLC Design	No	No	Yes
Status Communication to HMI	None	250 Milliseconds	250 Milliseconds
Status Update to C&C Chain-A from Chain-B	Hardwired	N/A	N/A
Status Update to C&C Chain-C from Chain-A & B	N/A	400 Milliseconds	30 Milliseconds
Chain-A EPICS Update time (Event Resolution Logging)	115.2 kb (2 Seconds)	N/A	N/A
Chain-B EPICS Update time (Event Resolution Logging)	19.2 kb (1 Second)	N/A	N/A
Chain-C EPICS Update time (Event Resolution Logging)	N/A	1.5 Mb (2 Milliseconds)	10 Mb (.2 Milliseconds)
Chain-C Processor	N/A	Industrial Computer	A/B Control Logics PLC
Software/Functionality			
Command and Control	Chain-A	Chain-C	Chain-C
Emergency Shut Down	Chain A & B	Chain A & B	Chain A & B
Invasive Testing	Chain-A & B	Chain-A & B & C	Chain-C
Non-Invasive testing	No	No	Chain-A & B
Automated Test Capability	No	Partial	Chain-A & B
Continuous Diagnostics (Output Point Level/Sensor Comparison)	No	Limited Chain-C	Chain-C
Minor, Serious and Major Fault Detection and Handling	Yes	Yes	No
Warning Detection (maintenance issues)	No	Yes	Yes
Minor and Major Fault Detection (No Serious Category)	No	No	Yes
Software Remote Shutter Operation	No	Yes - EPICS	Yes - EPICS
Data Logging/Status Resolution to EPICS	1-2 Seconds	2 Milliseconds	< 1 Second
Data Logging Local (All user and sensor inputs and system output)	No	1 Millisecond	No

The Features of The PSS

Generation-1

- **The Good Things**
  - It Works and it works well.
  - A considerable amount of software redundancy
    - *Less likely to fail due to a single error in code.*
  - It provides the expected safety functionality required by the SAD, DOE Guidance, ES&H and other applicable standards.
- **And the Bad things**
  - A considerable amount of software redundancy
    - *A lot of code to sort through to make a change in possibly several places.*
  - Non-Grounded System (Trouble shooting could be a problem).
  - Chain-A ESD also performed all Command and Control Functions.
  - Point-to-Point wiring.

The Features of The PSS

Generation-1

- **Lessens learned**
  - The design has both HMI and ESD functionality in Chain-A
    - *Changes in HMI code exposes the ESD code to unintentional modifications.*
    - *Each SCR requires extensive testing be done to the entire Chain-A software.*
  - Chain A faults created by un-commanded operations in Chain-B.
  - Chain-B must latch faults for diagnostic reasons.
  - Over 98% of PSS software change requests involved only HMI functionality not emergency shutdown tasks.
  - Better diagnostics from the system to shorted user down time.

The Features of The PSS

Generation-2

- **The Good Things**
  - Remove HMI functionality from Chain-A
    - *Reduced ESD code exposure to unintentional modifications.*
    - *SCRs involving only the Chain-C HMI do not require revalidation of Chain-A or Chain-B.*
  - Un-commanded Chain-B operations eliminated.
  - Chain-B latches all faults for diagnostic reasons.
  - More responsive to user request for change of the HMI.
  - Every operator action, all outputs to the beamline devices and all external permits are logged with millisecond resolution.
  - It is a more modular single point grounded system.
  - The EPICS interface is now bi-directional.
  - And it provides the expected safety functionality required by the SAD, DOE Guidance, ES&H and other applicable standards.

The Features of The PSS

Generation-2

- **And the Bad things**
  - The system got off to a shaky start with a large international vendor promising a single source solution.
  - We were promised production PLC components and delivered beta modules.
  - We were promised a well tested HMI with a large established user base. We received a HMI the factory experts couldn’t make work even though they were given months.
  - The users come to not trust the system.
  - It should be noted the problem areas affected only Chain-C and never compromised the ESD Chain-A and Chain-B systems. In fact the Chain-A and Chain-B systems used the same hardware as Generation-1 with enhancements to the code and communications.

The Features of The PSS

Generation-2

- **We learned some serious lessons**
  - Even international vendors that “Bring Good Things to Life” Have QC Problems.
  - Six Sigma (Bah Humbug) be sure it is not just marketing.
  - We replaced the failing components with product that had been used by the team members before and known to work.
  - Users working directly with the repaired system came to trust it quickly. However, other parties have been much slower to accept that it is now an easy to use and reliable system.
  - Moving parts in the Touch Screen computers are a problem.
  - Our two ESD system vendors informed us they would be retiring critical modules in our present design.

The Features of The PSS

Generation-3

- **The Good Things**
  - Non-Invasive Testing designed in.
  - Circuit Board replaces point-to-point wiring.
  - Updated to current PLC technology.
  - Chain-C monitoring of safety system redundant sensors providing continuous diagnostics, not normally available without using safety rated PLC. However, No safety credit taken.
  - Simplification of the safety code - more robust, secure, etc.
  - Chain-C provides the user interface - as a non-trusted system it is easier to accommodate user interface change requests. (95% of PSS code changes).
  - Provides the infrastructure for automated functional Validations.

The Features of The PSS

- **And the Bad things**
  - We will find out!

The Features of The PSS

- **Lessons learned**
  - This is a work sheet.

The Features of The PSS

QUESTIONS ?

Break

Non-Invasive Testing Methodology

Mike Fagan

Non-Invasive Testing Methodology

- **Overview**
  - The Validation process.
  - Problems exist with the testing methodology used in Generation 1 Systems.
  - Several solutions to those problems were considered.
  - Final solution includes the addition of diodes into the circuitry to overcome some of the problems.
  - Any potential problems with diodes will be addressed.
  - These changes to the testing methodology address and solve the shortcomings discovered with Generation 1 testing methods.

Validation process

- **Steps involved in validating a beamline**
  - Beamline is set to global offline.
  - Air supply is locked out/tagged out.
  - An I/O validation is preformed.
  - Functional test is preformed.
  - Air supply is enabled.
  - Beamline is set to global online.
  - End to end test performed.
- **Only changing functional testing step.**

Problems Presented During Validation

- **What problems exist?**
  - Front End Shutters
    - *Critical Devices – can't operate during validations.*
    - *Operations and statuses must be simulated.*
  - Other Systems
    - *May be offline.*
    - *Occasionally unavailable during validations.*
    - *Still must be tested.*

Problems Presented During Validation

- **What problems exist? (cont.)**
  - Testing requires removal of signals indicating safe conditions
    - *Signal activators physically inaccessible at times.*
    - *Cannot be made to read open without disassembly.*
  - All critical devices are monitored by both ESD chains and must be tested separately.

Current Testing Methodology

- **The Front End Rack Distribution Panel (FERDP) Simulator is connected**
  - The connectors on the FERDP are unplugged.
  - Simulator connectors are plugged in their place.
  - Allows the operator to manipulate and monitor the signals normally supplied by these devices and/or systems.
- **At each station user panel, a test box is used**
  - In order to facilitate specific test cases for critical devices, the Station User Panel connectors are unplugged.
  - A test box is plugged in series with the existing devices.
  - This test box is used to interrupt the signals from the field devices to simulate individual tests cases.

Problems with Current Testing Methodology

- **What problems exist in Gen 1 testing methodology?**
  - Disconnection of connectors is invasive.
  - Connectors may become damaged – difficult to detect.
  - Some critical devices are not being fully tested
    - *All possible cases not accounted for.*
    - *Only interruption of signals is tested.*
  - No provision for injection of signals for system tests
    - *Current method involves only manual tests on limit switches.*
    - *Current method potentially dangerous.*

Several Solutions Were Considered

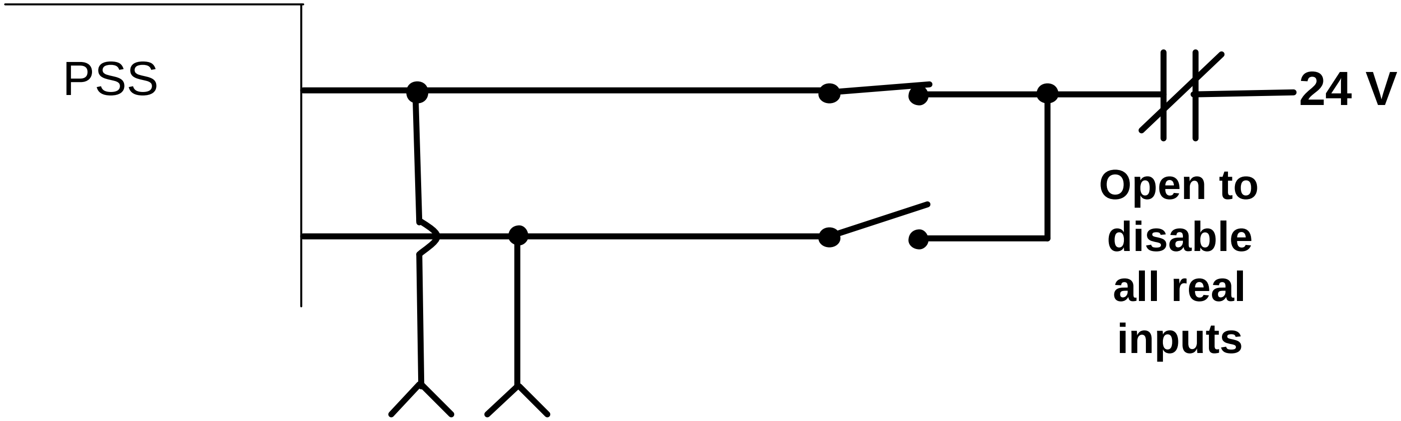
- **Possible solutions to testing problems:**
  - Relay in series with signal paths
    - *Only allows for signal interruptions.*
    - *Can’t verify contact was remade – mechanical device.*
  - SPST switch in series with signal paths
    - *Only allows for signal interruptions.*
    - *Can’t verify contact was remade – mechanical device.*
  - SPDT-center off switch in series with signal paths
    - *Could allow to forced-on signal as well as interruption.*
    - *Can’t verify contact was remade – mechanical device.*
  - All Solutions involve repeating steps for each signal on beamline.

Key Realizations Driving New Solution

- **What were they key realizations?**
  - Since all signals to ESD system are digital, all inputs could be disabled by removing power to field sensors.
  - Signal injection could be done on each and every signal.
  - Removal of a signal = no signal injected.
  - Signal injection could be done via connectors with hardware movable between beamlines.

Solution in its Basic Form

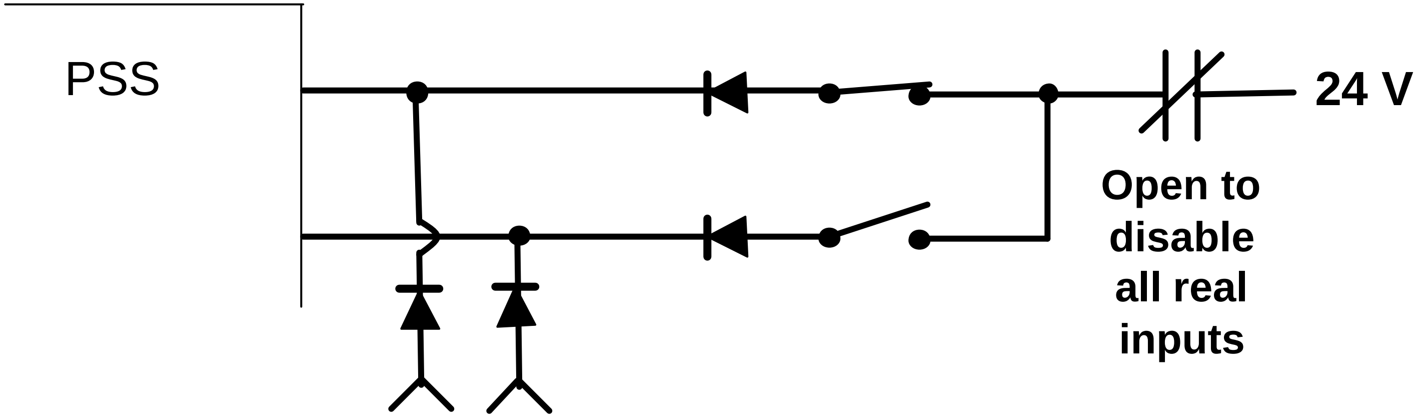
- **Solution chosen:**



Injected Test Signals

Solution in the Final Form

- **Solution not quite complete**
  - Basically a switch matrix.
  - Required diodes to allow for n-key rollover.
- **Final form:**



Injected Test Signals

Diodes – A New Component

- **Diodes are a key component for disabling the inputs**
  - Placed in series with the field device input signals.
  - Act as steering gates, allowing PSS to detect inputs from either. the field devices or from the injected signals.
- **Are there problems with adding diodes?**
  - How will failure effect the system?
  - How will we detect any diode failures?

Possible Failure Modes of the Diodes

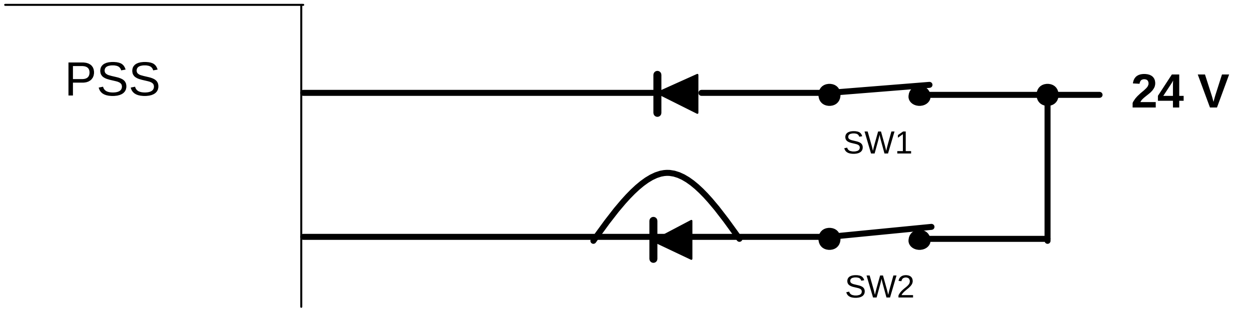
- **What are the ways that the diodes could fail?**
  - Resistive (due to digital nature of inputs, degenerates into either)
    - *Diode acts like short circuit.*
    - *Diode acts like fail opened.*
  - Shorted
  - Opened
  - Reversed
    - *Diode could be installed incorrectly.*
    - *Diode could be mislabeled.*

Diode Failure - Resistive Case

- **Since the inputs of the ESD system are digital – resistive failure will appear to be either an open or a short circuit**
  - If the resistance is low enough, there will be sufficient current to meet “true” logic threshold. This would act the same as having no resistance in series.
  - If resistance is too high, current will be limited to below threshold for “true” and the signal will be detected as “false.” This would act the same as having an open circuit.

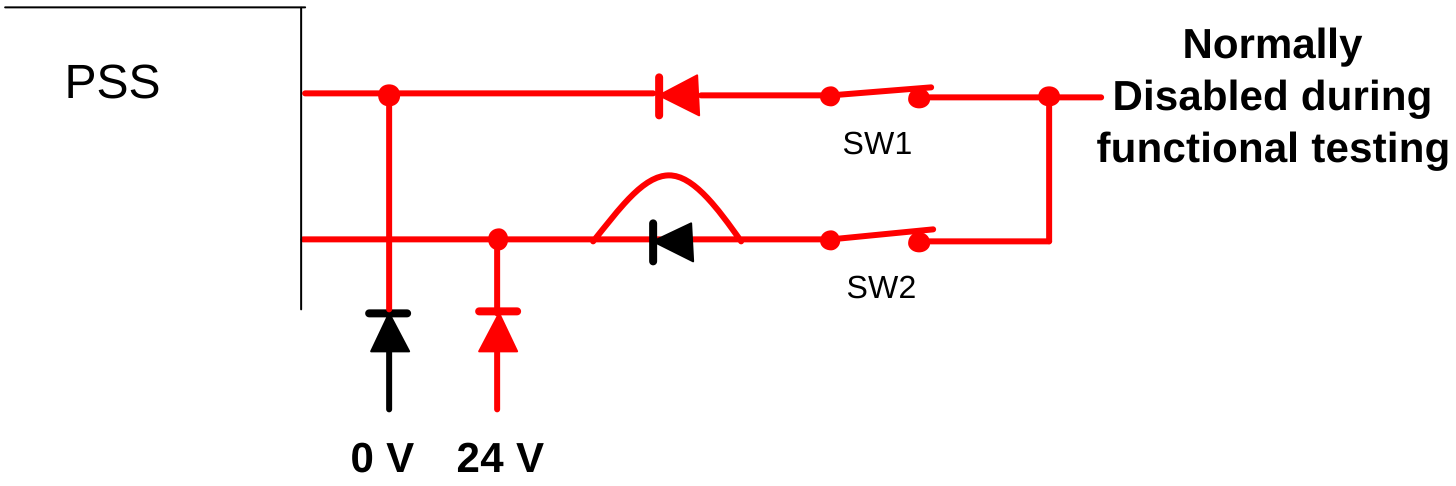
Effects of a Shorted Diode

- **PSS is in normal operation:**
  - Circuit functions as if the diode were never introduced.
  - The system continues to function as before.
  - PSS would see switches as open or closed irregardless of diode function.



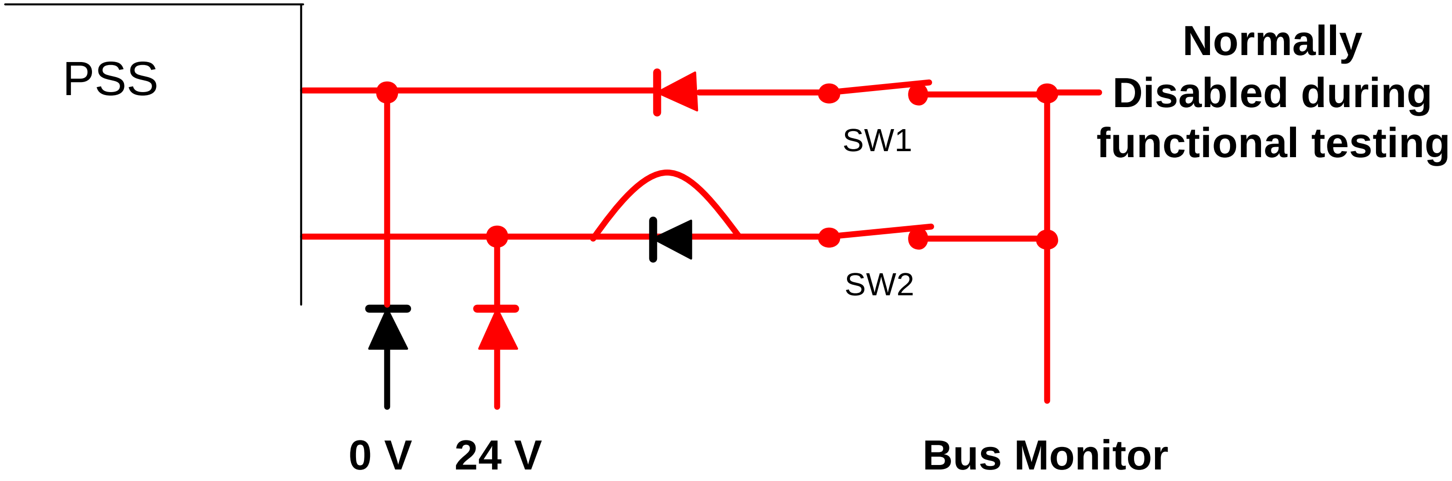
A Possible Problem

- **During functional test phase of validation, a problem could occur.**
  - Shorted diode could create a “sneak” path.
  - “Sneak” path would energize disabled power bus and allow an input not being injected to show a false true.
  - Functional testing would be flawed as result.



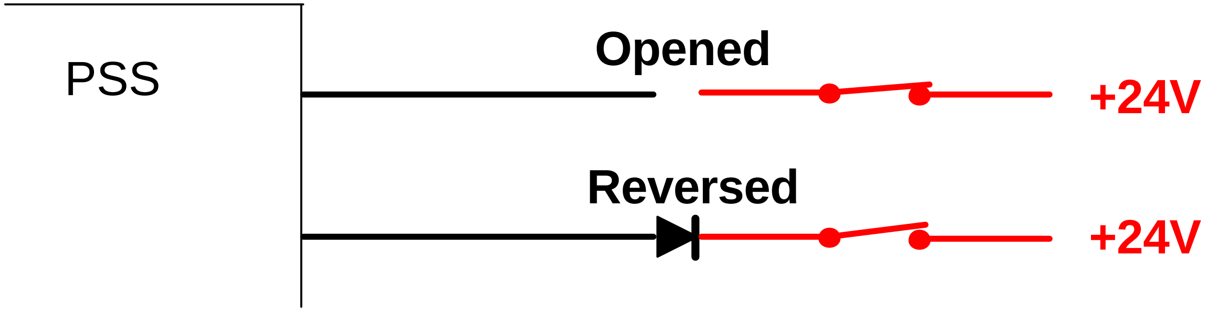
The Solution

- **Disabled common bus must be monitored**
  - If voltage is detected, the system “sees” the shorted diode.
  - Monitoring common bus associates the short with the specific signal being tested.



Effect of Either an Open or Reversed Diode

- **An open or reversed diode will be detected as the same**
  - I/O validation will detect lack of voltage on associated input.
  - Same result as any other open circuit that may occur.
- **Reversed diode will also cause the functional test to fail**
  - Seen in same way as shorted diode.
  - Detected by the bus monitor.



Addition of Diode is Failsafe

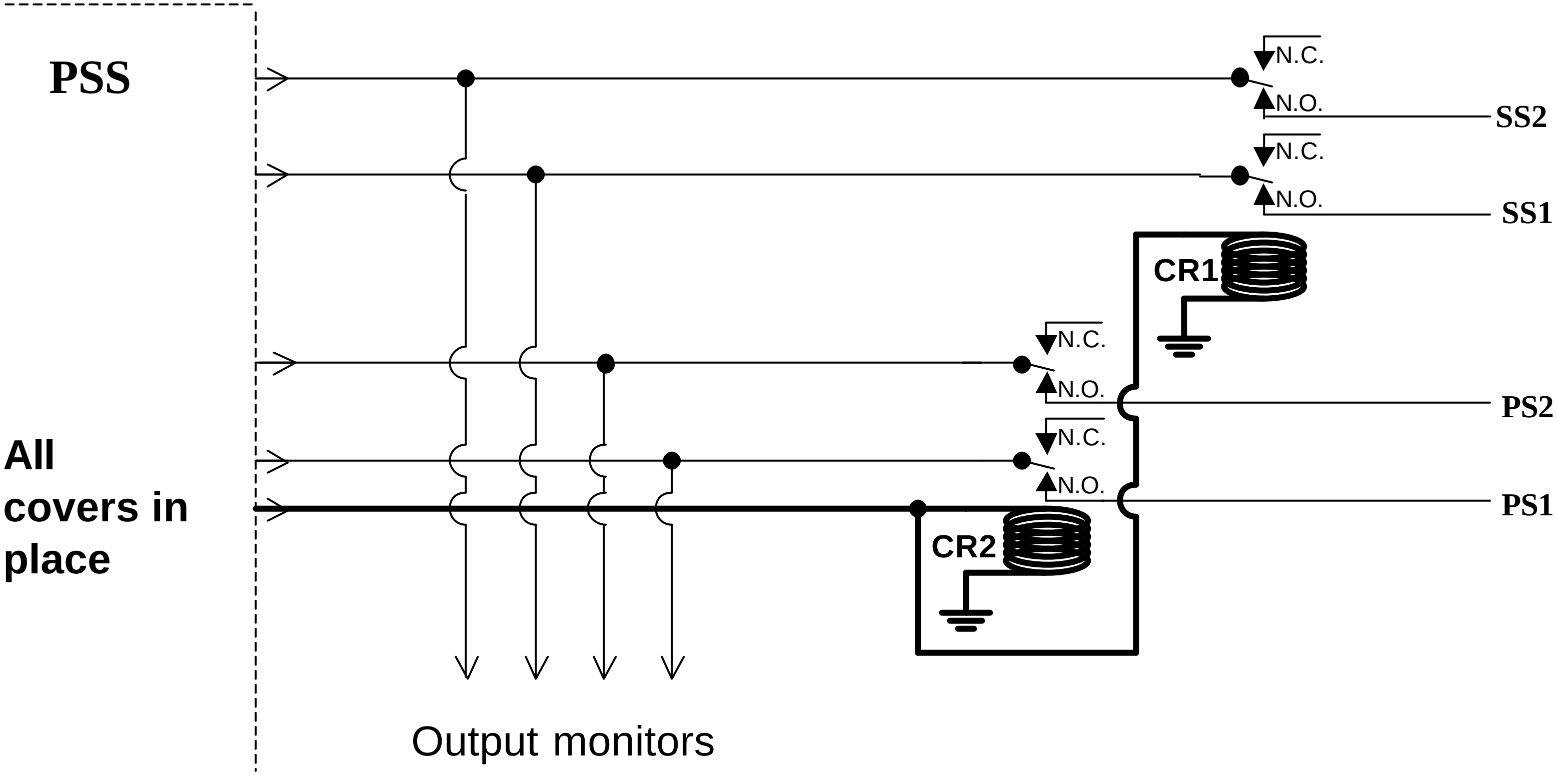
- **Addition of diodes to PSS keeps system failsafe**
  - In the event of a short, circuit acts the same as if circuit with no diodes.
  - In the event of an open or reversed diode, system treats it as any other open circuit, in a failsafe manner.
- **The diodes for the validation system do not affect the failsafe nature of the PSS**
  - During normal PSS operation, the validation system is unplugged and the diodes are not part of the circuit.

Safeguards

- **What safeguards would exist?**
  - Since signal injection would allow the validation system to inject false “safe” signals into the ESD system, safeguards are needed to prevent creating an real unsafe condition.
  - A hardwired function insures front end shutters are disabled whenever signal injection is possible
    - *Different hardwired function than global offline disable.*
    - *Hardwired function is in addition to locking out air supply.*
  - Signal injection connectors are protected by a cover
    - *Opening a cover disables final path to front end shutters.*
  - The hardwired function also removes the storage ring permits to ACIS.

Final Path to Front End Shutters

- As long as all covers remain in place, final path to the front end shutters is enabled.



Key Changes to Testing Methodology

- **Key Changes include:**
  - Front End Critical Devices disabled via relays – not unplugged.
  - Inputs treated consistently – control power disabled via relay.
  - Full functional test possible due to injection of signals.
  - No field devices are unplugged or disconnected for testing.
  - Critical devices are re-enabled after tests, not reconnected.
  - The disable method is failsafe.
  - Puts the groundwork in place for automation of the functional testing.
  - But, automation is not part of the current proposal.

Summary

- **Summary**
  - Problems existed with the testing methodology used in Generation 1 Systems.
  - Solutions to those problems were considered and discussed.
  - Final solution includes the addition of diodes into the circuitry to overcome some of the problems.
  - Potential problems with diodes were addressed.
  - The changes to testing methodology address and solve the shortcomings discovered with Generation 1 testing methods, and allow for more complete testing in Generation 3 systems.

Non-Invasive Testing Methodology

QUESTIONS?

Generation 3 Hardware Design

Ken Belcher

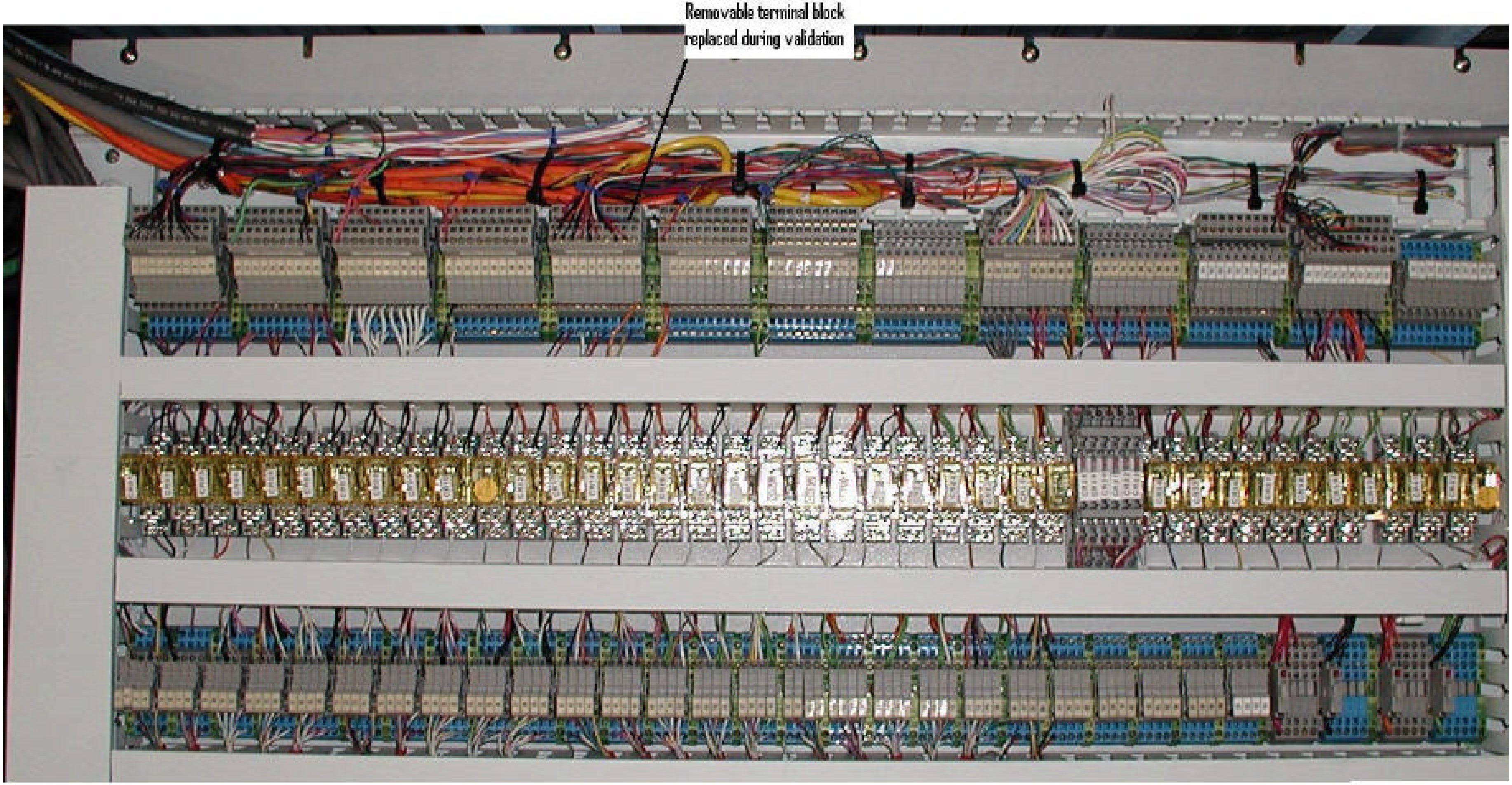
PSS Generation 3 Hardware Overview

- Highlight changes from Generation 1 and Generation 3.
- Review all external interfaces.
- Discuss key internal safety related circuits.
- Review Validation System interface to the Generation 3 PSS.

PSS Hardware Generation 3 vs. Generation 1

- **What components/system/methods are <u>unchanged</u>**
  - Two redundant ESD PLC systems needed to permit all safety related outputs and to monitor all safety related inputs.
  - Watchdog timers allow each ESD PLC to monitored each other.
  - All external systems interface to the PSS thru isolation relays.
  - All I/O are failsafe (i.e. de-energized = safe).
  - All Generation 1 field devices and their interfaces remain.
  - Physical (manual) I/O validation to verify the actual source and destination of PLC I/O (i.e. wiring checkout).
  - Emergency Egress system inside hutches independent of logic.

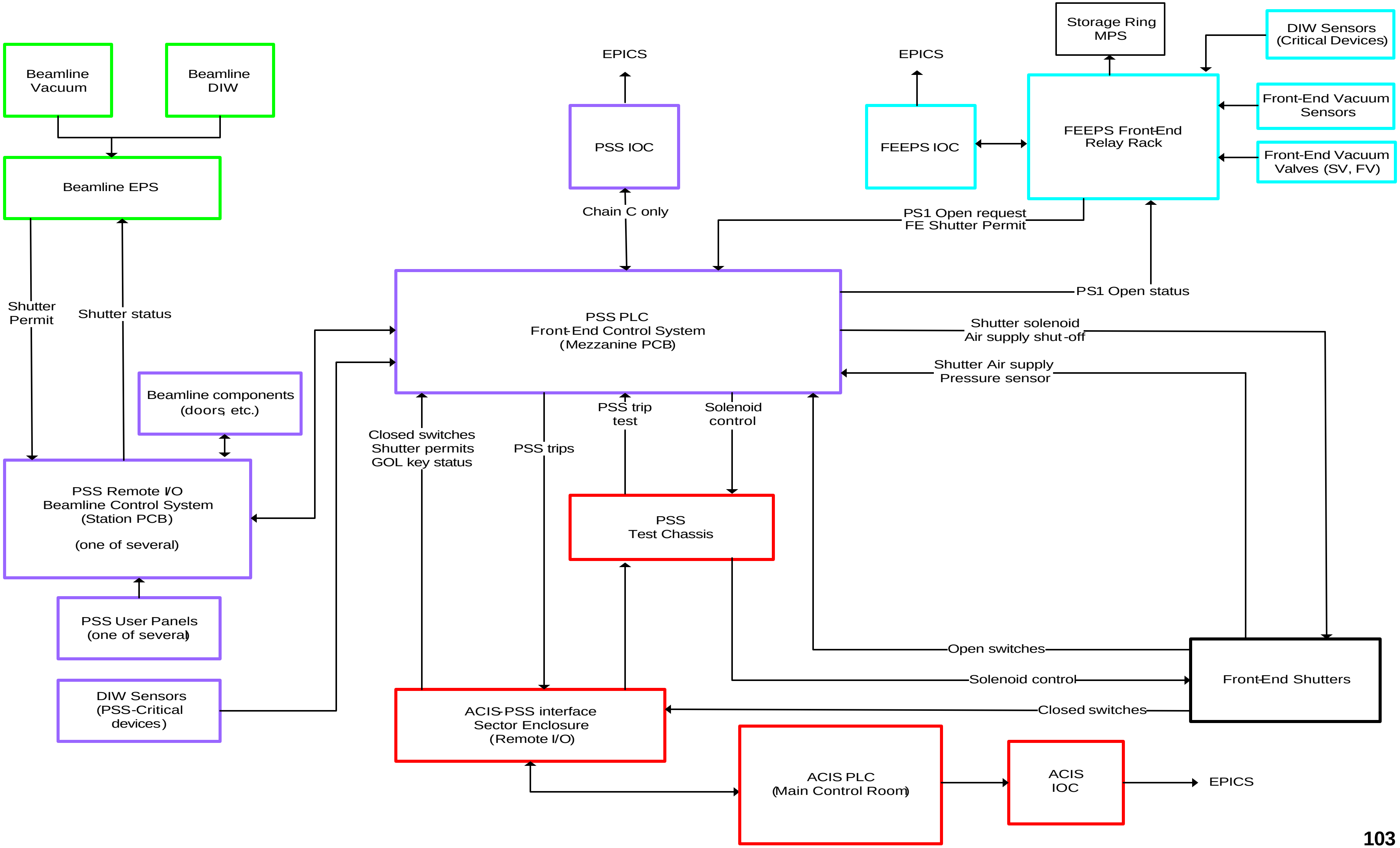
PSS Ver. 1 Front End Relay Distribution Rack


Removable terminal block replaced during validation

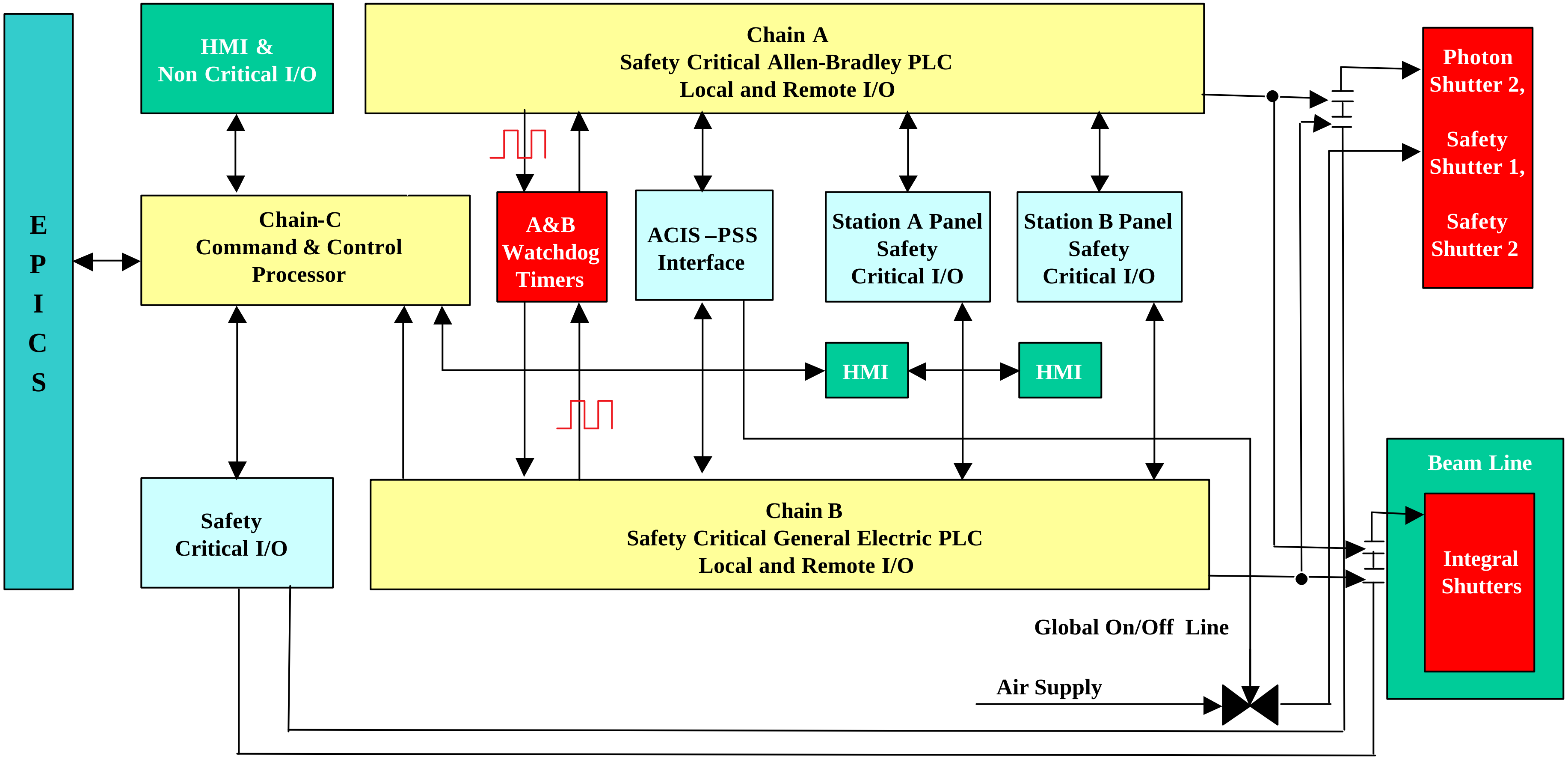
PSS Hardware Generation 3 vs. Generation 1

- **What components/system/methods are <u>changed</u>**
  - Newer versions of Chain A and B PLCs.
  - Direct Chain A to Chain B Watch Dog Timer interface.
  - Third PLC for command, control, logging and communications
    - *Chain C commands are executed only if A and B permit.*
    - *Chain C has no ESD responsibility.*
    - *Chain C code, for the user interface, can be altered without requiring revalidation of ESD code (Most software changes historically have been with regards to the user interface).*
  - <u>Full functional non-invasive validation of ESD PLCs (A & B).</u>

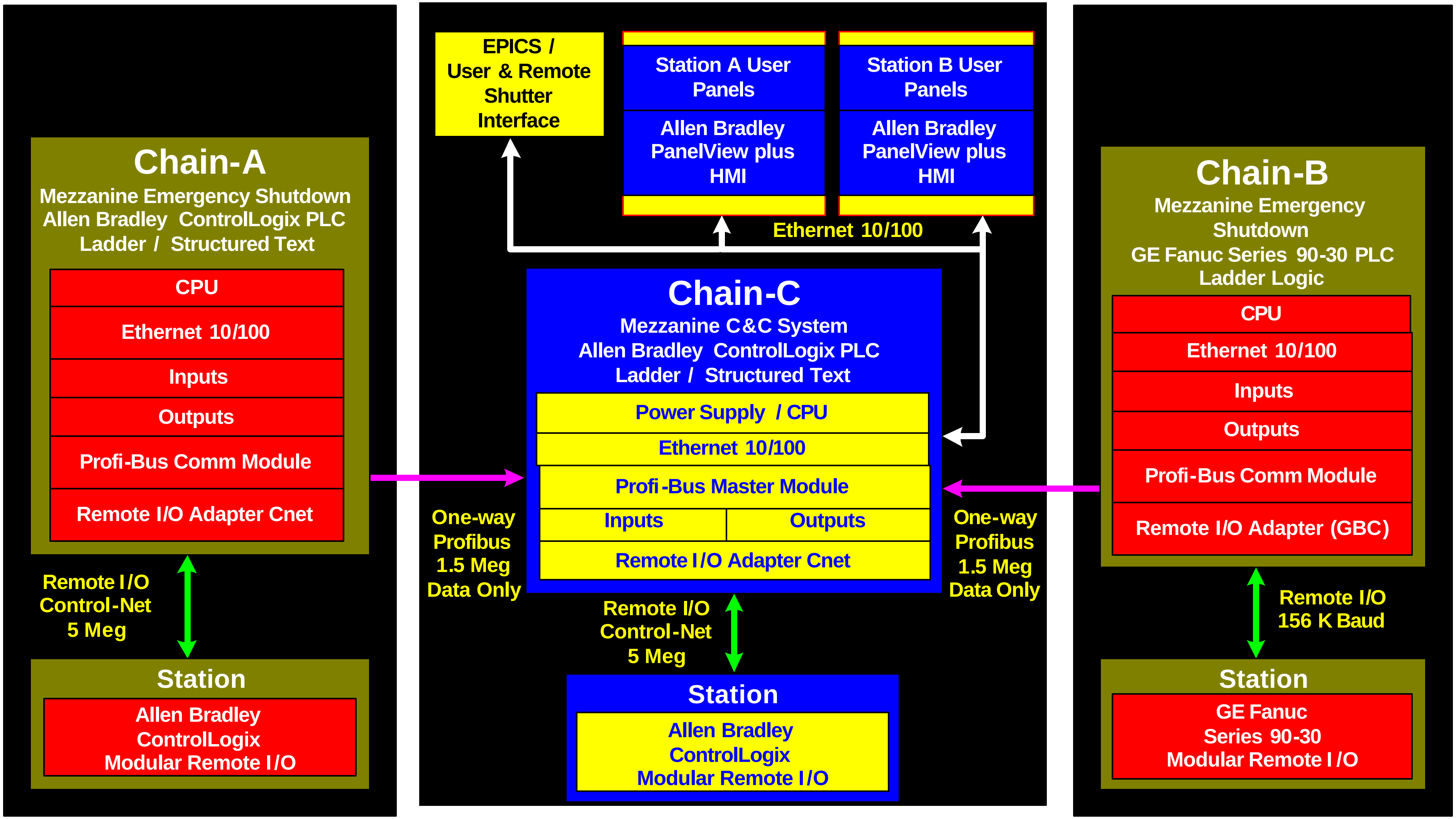
PSS Gen. 3 overview of external interfaces



PSS Generation 3 hardware system overview



PSS Generation 3 communications overview



EPICS / User & Remote Shutter Interface

Station A User Panels

Allen Bradley PanelView plus HMI

Station B User Panels

Allen Bradley PanelView plus HMI

Ethernet 10/100

Chain-A

Mezzanine Emergency Shutdown
Allen Bradley ControlLogix PLC
Ladder / Structured Text

- CPU
- Ethernet 10/100
- Inputs
- Outputs
- Profi-Bus Comm Module
- Remote I/O Adapter Cnet

Remote I/O
Control-Net
5 Meg

Station

Allen Bradley
ControlLogix
Modular Remote I/O

Chain-C

Mezzanine C&C System
Allen Bradley ControlLogix PLC
Ladder / Structured Text

- Power Supply / CPU
- Ethernet 10/100
- Profi-Bus Master Module
- Inputs | Outputs
- Remote I/O Adapter Cnet

One-way
Profibus
1.5 Meg
Data Only

Remote I/O
Control-Net
5 Meg

Station

Allen Bradley
ControlLogix
Modular Remote I/O

One-way
Profibus
1.5 Meg
Data Only

Chain-B

Mezzanine Emergency Shutdown
GE Fanuc Series 90-30 PLC
Ladder Logic

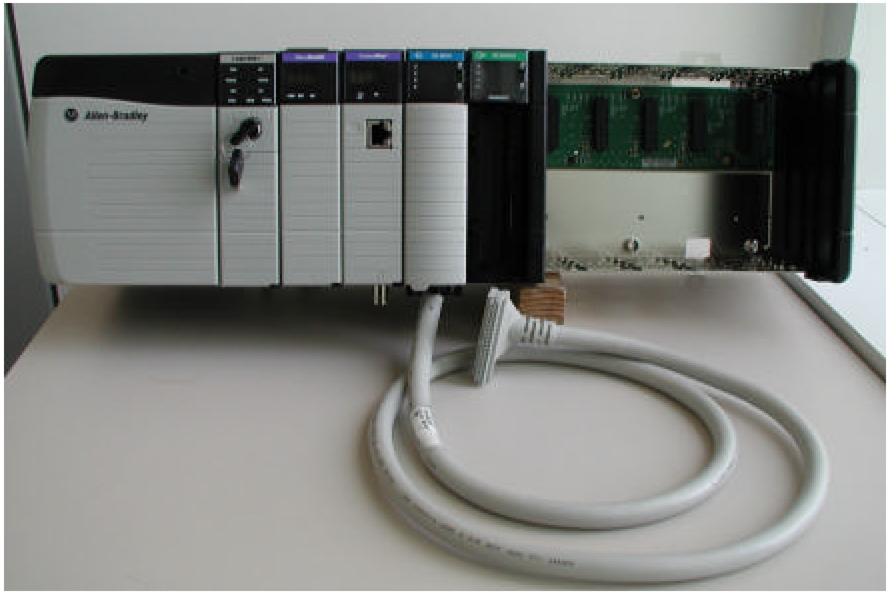
- CPU
- Ethernet 10/100
- Inputs
- Outputs
- Profi-Bus Comm Module
- Remote I/O Adapter (GBC)

Remote I/O
156 K Baud

Station

GE Fanuc
Series 90-30
Modular Remote I/O

PSS Generation 3 – Newer PLCs



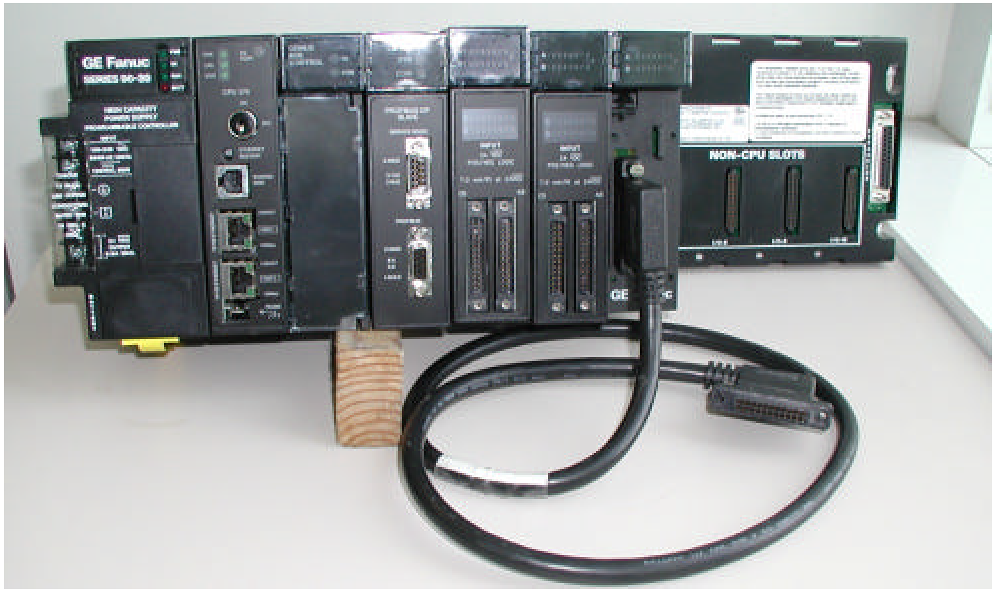
Allen-Bradley Contrologix system

1756-L61 Processor

1756-CNB Control-Net module for Remote I/O

1756-ENBT Ethernet module for programming port only

SST-PFB-CLX Profibus module for data out to Chain C



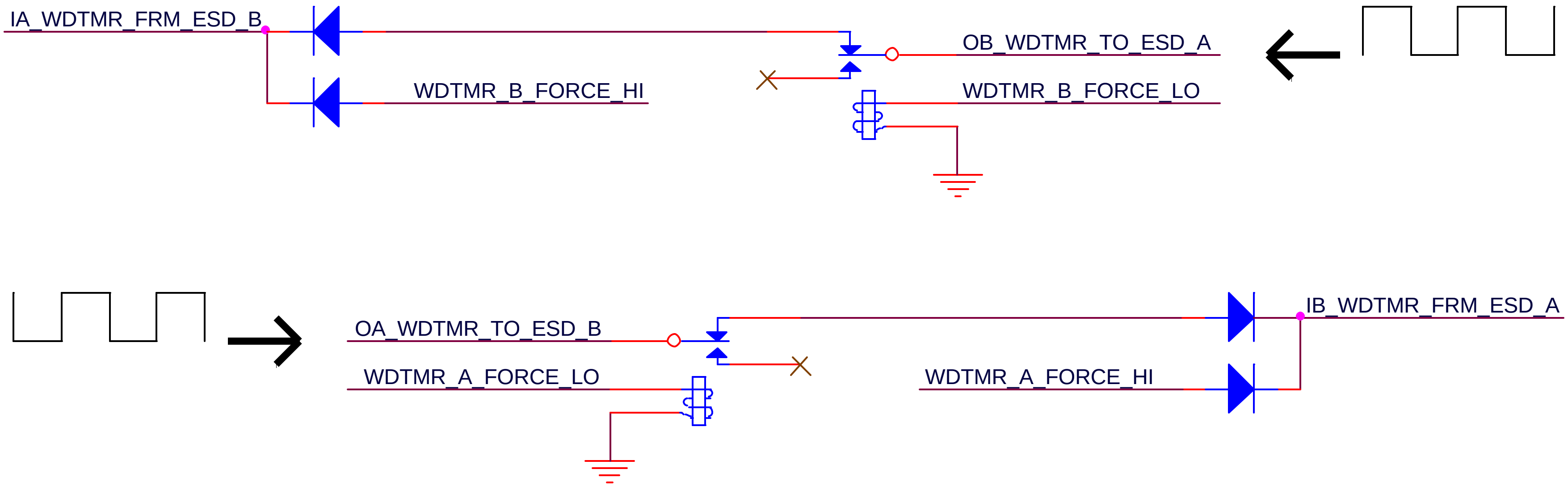
General Electric GE Fanuc 90-30 system

IC693CPU374 Processor w/Ethernet

IC693BEM331 Genius Bus for Remote I/O

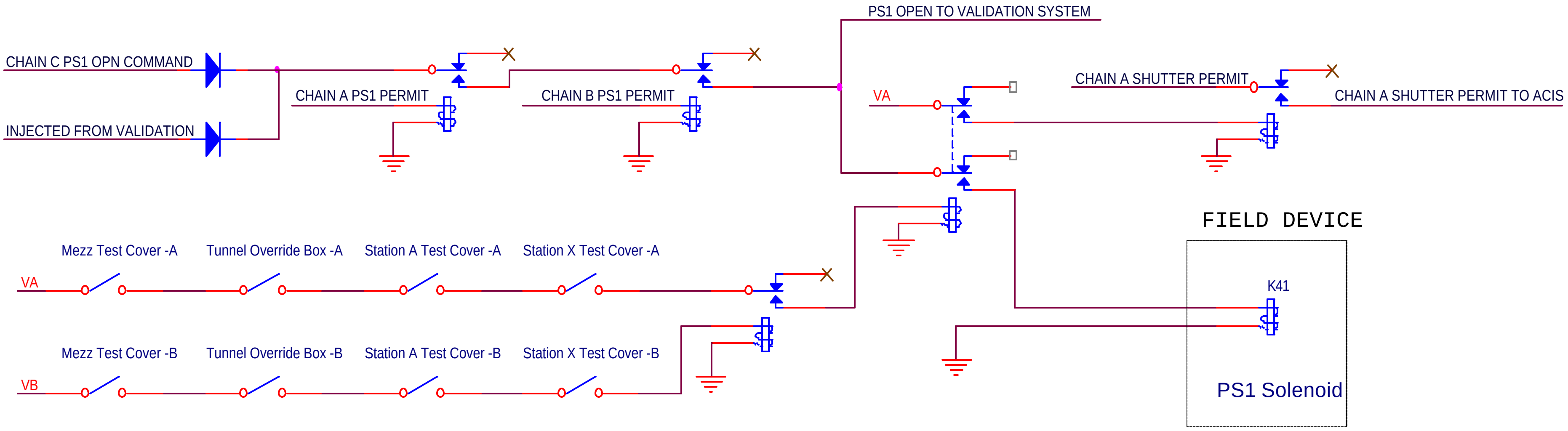
IC693PBS201 Profibus module

Watch Dog Timer Circuit



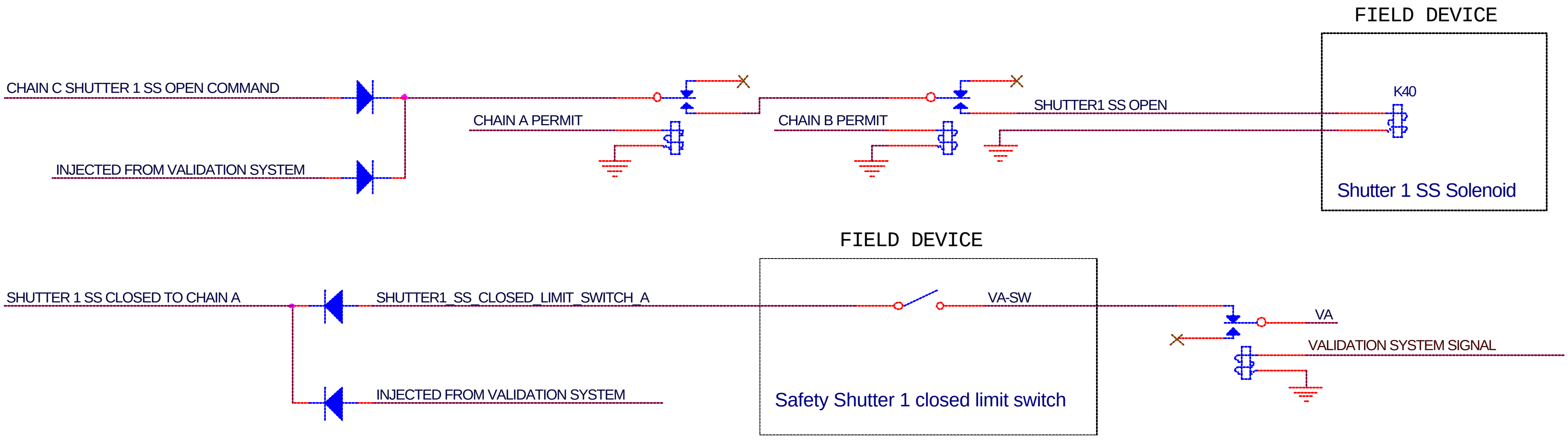
- **OA_WDTMR_TO_ESD_B is a Chain A output pulse train read by Chain B.**
- **OB_WDTMR_TO_ESD_A is a Chain B output pulse train read by Chain A.**
- **To simulate a Watchdog timer open circuit or zero, the validation system will inject FORCE_LO .**
- **To simulate a Watchdog timer stuck in the ON state, the validation system will inject FORCE_HI.**

Hardwired Front End Shutter shutdown logic



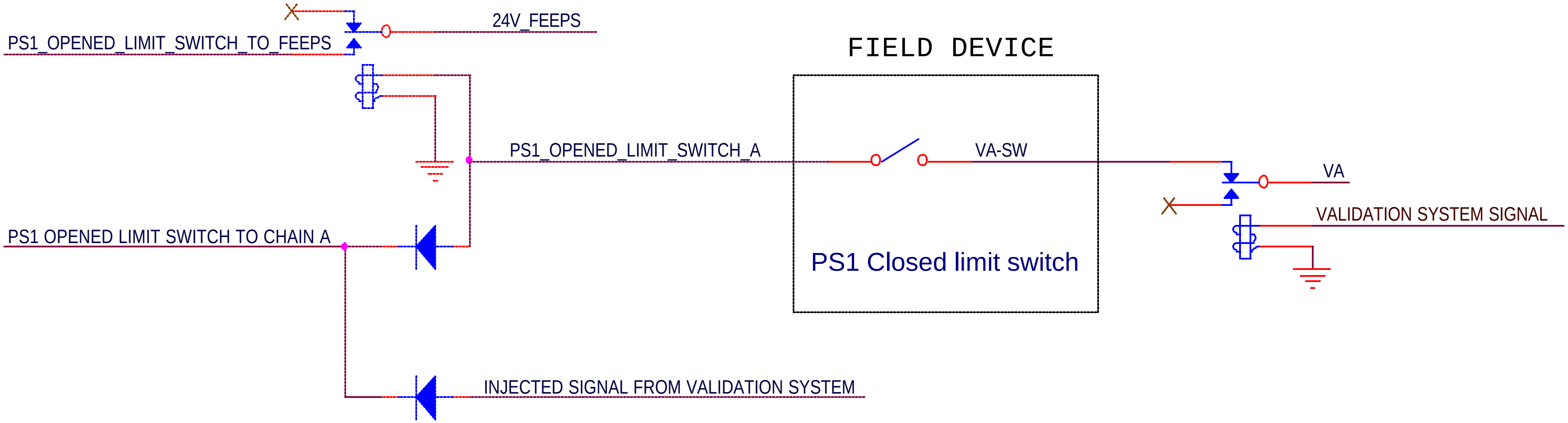
- Chain C OPEN command needs Permit signals from Chain A & B to energize the solenoids.
- DPDT relay will de-energize Front End Shutter solenoids through hardware if a Test Cover is accessed.
- SHUTTER PERMIT signal is removed to ACIS, which adds an additional layer of protection.
- During Validation, Validation system injects an OPEN command and monitors results after Chain A & B permits.

Integral Beamline Shutter Control System


FIELD DEVICE
CHAIN C SHUTTER 1 SS OPEN COMMAND
CHAIN A PERMIT
CHAIN B PERMIT
SHUTTER1 SS OPEN
K40
INJECTED FROM VALIDATION SYSTEM
Shutter 1 SS Solenoid
FIELD DEVICE
SHUTTER 1 SS CLOSED TO CHAIN A
SHUTTER1_SS_CLOSED_LIMIT_SWITCH_A
VA-SW
VA
VALIDATION SYSTEM SIGNAL
INJECTED FROM VALIDATION SYSTEM
Safety Shutter 1 closed limit switch

- **Chain C OPEN command needs Permit signals from Chain A & B to energize the solenoids.**
- **During Validation the Validation system first disables field device power source.**
- **Second the Validation system can inject proper signals to simulate field devices.**
- **VA-SW is then monitored by the Validation system at all times making sure no voltage is present indicating a wiring error or diode failure.**

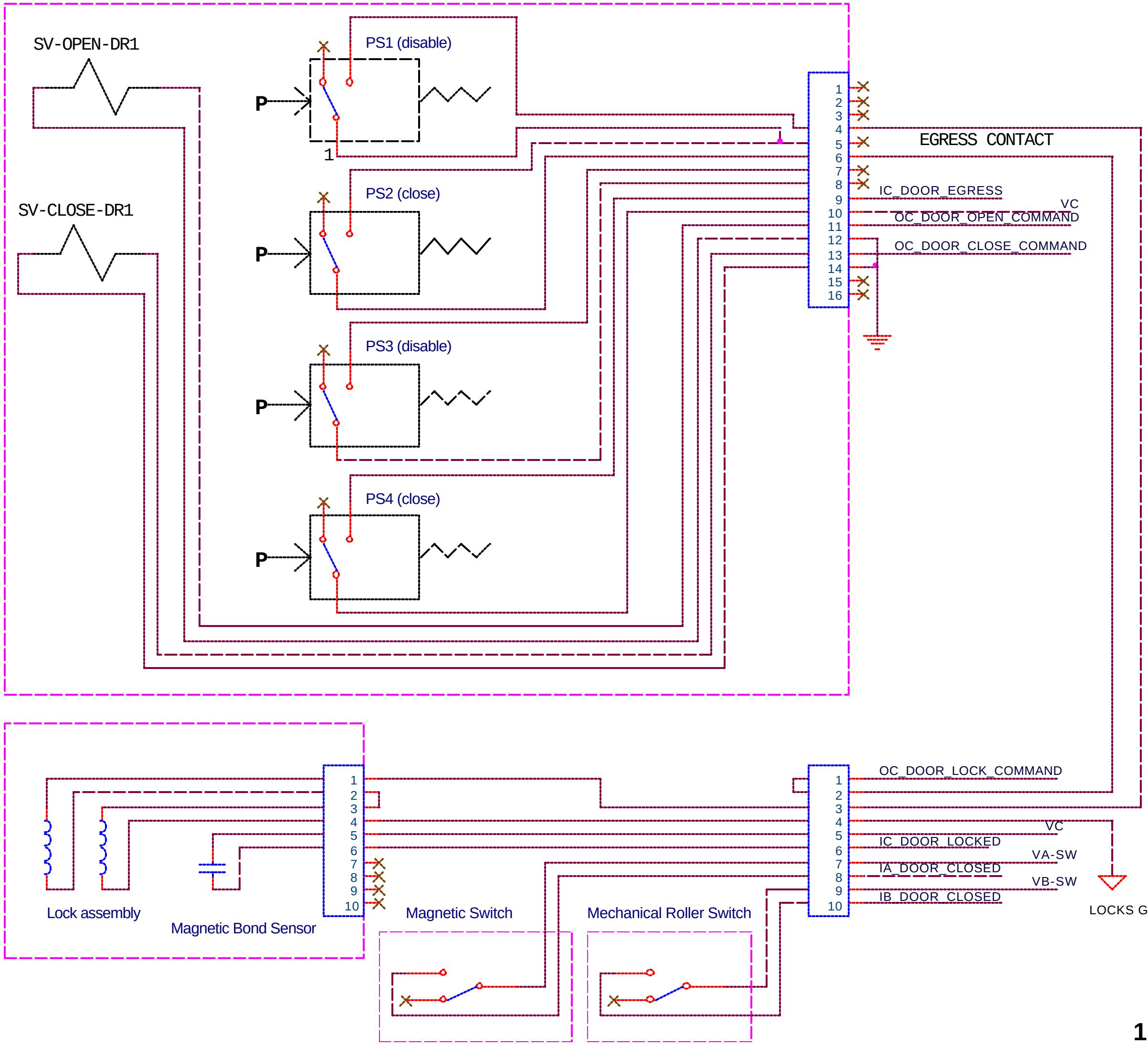
Front End EPS (FEEPS) Interface


24V_FEEPS
PS1_OPENED_LIMIT_SWITCH_TO_FEEPS
FIELD DEVICE
PS1_OPENED_LIMIT_SWITCH_A
VA-SW
VA
VALIDATION SYSTEM SIGNAL
PS1 OPENED LIMIT SWITCH TO CHAIN A
PS1 Closed limit switch
INJECTED SIGNAL FROM VALIDATION SYSTEM

- **Front End Shutter OPEN limit switch A is sent to Chain A and to FEEPS thru relay isolation.**
- **During Validation the Validation system first disables field device power source.**
- **Second the Validation system can inject proper signals to simulate field devices.**
- **VA-SW is then monitored by the Validation system at all times making sure no voltage is present indicating a wiring error or diode failure.**

Pneumatic Door Control

- The Door Open Command is generated by a Chain C output through Chain A & B Permits.
- The resulting signal can only operate the lock when PS2 is sensing proper air pressure.
- Chain C sees the air pressure to close the door is adequate thru PS4 and the magnetic force is available at the lock.
- Chain A sees a magnetic position switch is made if the door is physically closed.
- Chain B sees a mechanical position switch under the same conditions.



Validation System for Non-invasive Testing

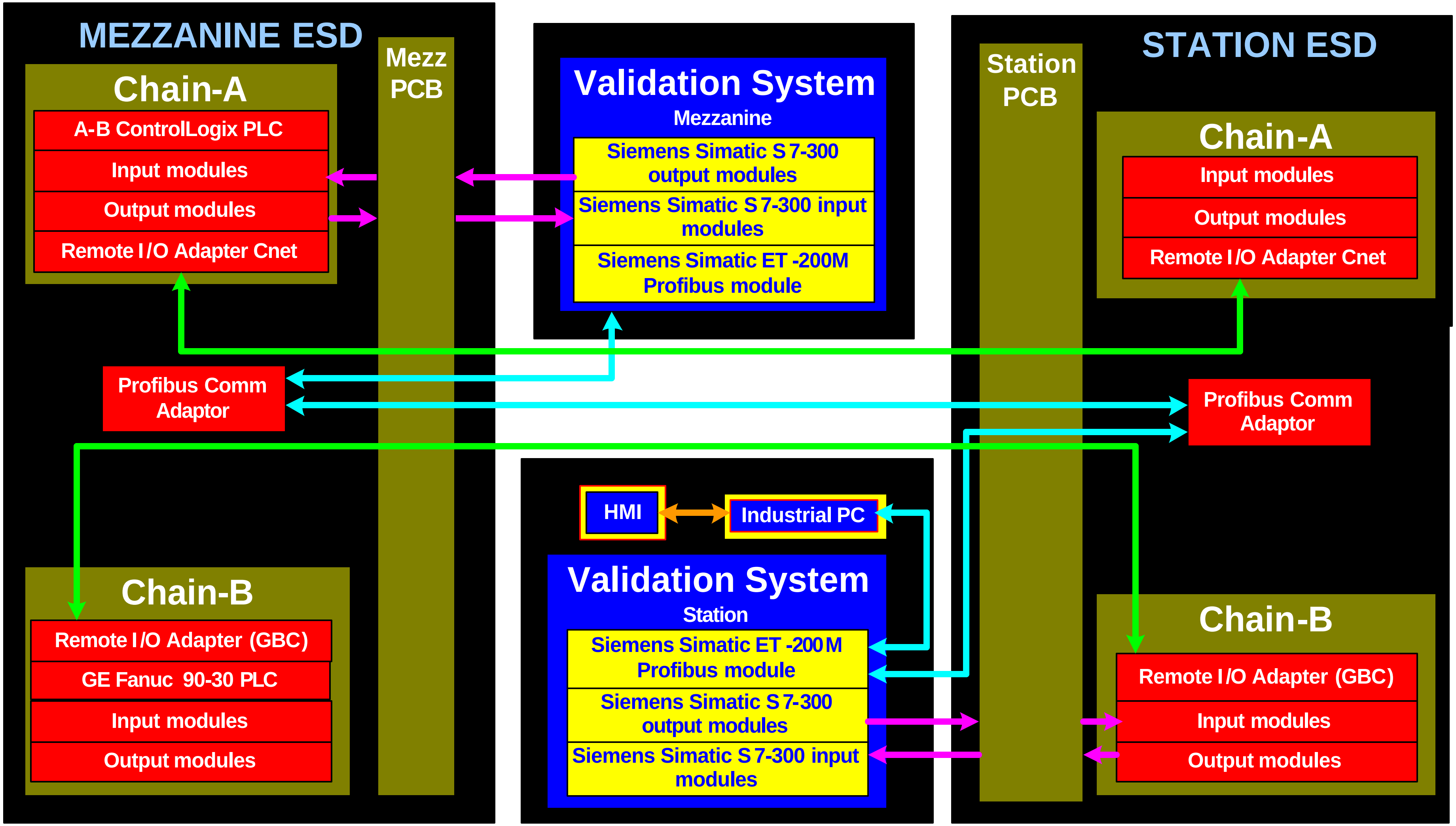
- **The Validation system hardware will only interface with the ESD systems, Chain A and Chain B.**

- **The Validation system I/O will connect to 120 pin connectors on pigtails which will connect directly to the PSS PCB's only after the Test Cover is open.**

- **The Validation system I/O will obtain power from the PSS PCB and proceed to disable actual field devices to prepare to inject these signals.**

- **The Validation system is modular and designed to be easily validated with simple point to point techniques.**

Validation system connection to PSS overview



Validation System Hardware

- PC Based Control System
  - *Integrating Siemens Distributed I/O.*
  - *Open Architecture - Multiple Hardware Vendors.*
- Modular, Easily Expandable.
- Hi-performance 2 Millisecond Scan Time
  - *Test Race Conditions.*
  - *Data Logging For Testing Accuracy & Analysis.*
- Capacity For Future Automated Testing.
- Have History With Hardware & Software
  - *Beamline 04-ID and Gen-1 Beamline Simulator.*
- Our System Of Choice For The Application.

Generation 3 Hardware Design

QUESTIONS?

Lunch